



EdgeSight

Contents

EdgeSight	9
EdgeSight 5.4	10
EdgeSight 5.4	11
About	12
New Features for EdgeSight 5.4	14
Known Issues in EdgeSight 5.4	16
Fixed Issues in EdgeSight 5.4	18
System Requirements	19
Install	30
Installing EdgeSight Server	35
Installing EdgeSight Server Using the User Interface	37
Installing EdgeSight Server Using the Command Line	40
Running the Post-Installation Setup Wizard	43
Installing EdgeSight Agents	46
Installing an Agent Using the User Interface	48
Installing EdgeSight Agents Using the Command Line	50
Installing the EdgeSight for XenApp Agent in a Streamed Environment	57
Configuring Agents Using the Control Panel	60
Installing EdgeSight for Monitoring Virtual Desktops	62
Configuring Database Brokers	64
Installing the Agent Database Server	65
Setting Up the Agent Data File Share	67
Prerequisites for Installing EdgeSight Agents	70
Installing the Agent	72
Deploying the Agent to Virtual Desktops in a Pool	76
Post-Installation Configuration	78
Installing EdgeSight Active Application Monitoring Software	80
Configuring Third Party Software	83

Upgrade	85
Manage	88
Terms and Concepts	93
Agent Types and Processes	94
Administrative Tasks and Roadmap	99
Managing Company Settings	101
Managing User Profiles	102
Managing Company Properties	103
Managing Departments, Devices, and Groups	105
Managing User Groups	108
Managing Roles	109
Managing Access to XenApp Farms	110
Creating Alert Rules and Actions	111
Managing Application Categories and Vendors	119
Managing Reports	120
Managing IP Ranges	121
Managing Real-Time Dashboard Configurations	122
Setting Agent Properties	123
Configuring, Scheduling, and Running Workers	126
License Server Monitoring	130
Managing Server Settings	132
Monitoring Server Status	133
Configuring Server Settings	134
Creating Companies	138
Managing Licenses	139
Managing Authentication Providers	144
Configuring Reporting Services	145
Managing the Database	146
Managing Maintenance Jobs	149
Handling Unmanaged Devices	150
Displaying Agent Database Broker Status	151
Displaying and Responding to Server Messages	153
Managing Server Scripts	154
EdgeSight Feature Availability	155
EdgeSight Feature Availability By Agent Type	156
EdgeSight Feature Availability By Agent Version	169
Data Collection by Presentation Server or XenApp Server Version	171

Integrate	178
System Requirements for EdgeSight Alert Integration with System Center Operations Manager	180
Installing and Configuring Components	182
Using the Management Pack	184
Security Considerations	189
Troubleshoot	191
EdgeSight 5.3 for XenApp	194
EdgeSight 5.3	195
About EdgeSight 5.3	196
New Features for EdgeSight 5.3	198
Known Issues in EdgeSight 5.3	202
Fixed Issues in EdgeSight 5.3	204
System Requirements for EdgeSight 5.3	205
Install and Configure	216
Installing EdgeSight Server	221
Installing EdgeSight Server Using the User Interface	223
Installing EdgeSight Server Using the Command Line	226
Running the Post-Installation Setup Wizard	229
Installing EdgeSight Agents	232
Installing an Agent Using the User Interface	234
Installing EdgeSight Agents Using the Command Line	236
Installing the EdgeSight for XenApp Agent in a Streamed Environment	243
Configuring Agents Using the Control Panel	246
Installing EdgeSight for Monitoring Virtual Desktops	248
Installing EdgeSight Server	250
Installing the Agent Database Server	251
Setting Up the Agent Data File Share	253
Prerequisites for Installing EdgeSight Agents	256
Installing the Agent	258
Deploying the Agent to Virtual Desktops in a Pool	262
Post-Installation Configuration	264
Installing EdgeSight Active Application Monitoring Software	266
Configuring Third Party Software	269
Upgrading EdgeSight	271
Managing EdgeSight	274
Terms and Concepts	279

Agent Types and Processes	280
Administrative Tasks and Roadmap	285
Managing Company Settings	287
Managing User Profiles	288
Managing Company Properties	289
Managing Departments, Devices, and Groups	291
Managing User Groups	294
Managing Roles	295
Managing Access to XenApp Farms	296
Creating Alert Rules and Actions	297
Managing Application Categories and Vendors	305
Managing Reports	306
Managing IP Ranges	307
Managing Real-Time Dashboard Configurations	308
Setting Agent Properties	309
Configuring, Scheduling, and Running Workers	312
License Server Monitoring	316
Managing Server Settings	318
Monitoring Server Status	319
Configuring Server Settings	320
Creating Companies	324
Managing Licenses	325
Managing Authentication Providers	330
Configuring Reporting Services	331
Managing the Database	332
Managing Maintenance Jobs	335
Handling Unmanaged Devices	336
Displaying Agent Database Broker Status	337
Displaying and Responding to Server Messages	339
Managing Server Scripts	340
EdgeSight Feature Availability	341
EdgeSight Feature Availability By Agent Type	342
EdgeSight Feature Availability By Agent Version	355
Data Collection by Presentation Server or XenApp Server Version	356
Integrating EdgeSight Alerts with Microsoft System Center Operations Manager	363
System Requirements for EdgeSight Alert Integration with System Center Operations Manager	365

Installing and Configuring Components	367
Using the Management Pack	369
Security Considerations	374
Troubleshooting EdgeSight	376
EdgeSight for Load Testing 3.8	379
EdgeSight for Load Testing 3.8	380
About EdgeSight for Load Testing 3.8	381
System Requirements for EdgeSight for Loading Testing 3.8	384
Installation Overview	386
Citrix EdgeSight for Load Testing Licensing	388
To Install the EdgeSight for Load Testing Components	389
To Install the Web Interface Support Components	390
Upgrading EdgeSight for Load Testing Components	391
Removing the Web Interface Components	392
Administer	393
Initial Configuration	394
Configure Servers	395
Ending Sessions Automatically	396
Setting User Session Limit	397
Setting Published Applications Settings	398
Setting Seamless Logins	399
Configure XenDesktop Environment	400
Configure Launchers	401
Disabling System Beep	402
Configure Controllers	403
Configure License Server	404
Create a Script	405
Concurrency Model	406
Create a Connection	409
Connecting with an ICA File	410
Connecting with the XML Service	411
Connecting with the Web Interface	412
Web Interface Access Credentials	414
Connecting to the Server Desktop	415
Create Users	416
View and Copy Users	417
Recording a Script	418

Strategy for Creating Good Scripts	419
Starting a Recording	420
Stopping a Recording	422
Replaying a Recording	423
Using Fast Record	424
Editing Scripts	425
Introduction to Script Editing	426
Navigation	428
Adding Instructions	429
Moving Instructions	430
Using Folders	431
Repeating Folders	432
Iterating Folders	433
Conditional Folders	434
Do Until Satisfied Example	435
Creating Conditional Folders	436
Folder Properties	437
Synchronization Points	438
Match Synchronization Points	440
Search Synchronization Points	441
Editing Keyboard Input	443
Keyboard Examples	444
Editing Mouse Input	446
Creating Variables	448
Importing Variables	450
Using Microsoft JScript	451
Supported Built-in JScript	452
User.SetSpeed() Example	453
Running a Load Test	454
Creating a Load	455
Concurrency Control	456
Rate Control	457
Add a Load	458
Adding Load Control Rules	459
Starting a Test	461
Viewing the Test Windows	462
Replaying a Test in Debug Mode	463

Stopping a Test	464
Scheduling Tests	465
Displaying Test Results	466
Displaying Script Performance	468
Connections Window	470
Counters Window	471
Add Windows Counter	472
Add Xen Counter	473
Delete Counter	474
Load Control Rule Window	475
Delete Load Control Rule	476
Alarms Window	477
Add Alarm	478
Delete Alarm	479
Measurement Window	480
Monitor Window	481
Messages Window	482
Chart Reports	483
Virtual Keys Reference	484
Creating an ICA File	486
Creating ICA Files for Versions Prior to Presentation Server 4.5	487
Creating ICA Files for Presentation Server 4.5 and Later	488
Creating ICA Files from the APPSRV.ini File	489
Script Example	491
Close Existing Doc Folder	492
Word Task Folder	493
Exit App Folder	495
Intelligent Load Control Example	496
Sample Load Control Rule	497
Sample Chart Report	499
Load Test Chart Report	500
Load Control Rule Runtime Activation Messages	501

EdgeSight

Citrix® EdgeSight™ is a performance and availability management solution for XenDesktop, XenApp and endpoint systems. EdgeSight monitors applications, devices, sessions, license usage, and the network in real time, allowing users to quickly analyze, resolve, and proactively prevent problems.

Product documentation is available for the following EdgeSight releases:

- [EdgeSight 5.4](#)
- [EdgeSight 5.3](#)

Quick Links

- [About EdgeSight 5.4](#)
- [System Requirements for EdgeSight 5.4](#)
- [About EdgeSight 5.3](#)
- [System Requirements for EdgeSight 5.3](#)
- [Install and Configure](#)
- [Manage](#)
- [Upgrade](#)
- [Integrate](#)
- [Troubleshooting](#)

EdgeSight 5.4

Citrix® EdgeSight™ is a performance and availability management solution for endpoint, XenDesktop, and XenApp systems. EdgeSight monitors applications, devices, sessions, license usage, and the network in real time, allowing users to quickly analyze, resolve, and proactively prevent problems.

In This Section

Under this node, you will find the following resources for EdgeSight:

About EdgeSight	An overview of EdgeSight and its features
New Features for EdgeSight 5.4	New features in this release
Known Issues in EdgeSight 5.4	Known issues in this release
Fixed Issues in EdgeSight 5.4	Fixed issues in this release
System Requirements for EdgeSight 5.4	System requirements for this release
Install and Configure	Installation procedures for all EdgeSight components
Upgrading EdgeSight	Upgrade and uninstallation procedures
Managing EdgeSight	Component and configuration information
Integrating EdgeSight Alerts with Microsoft System Center Operations Manager	How to use EdgeSight with Microsoft System Center Operations Manager
Troubleshooting EdgeSight	Information on troubleshooting license server monitoring and agent log files

Can't find what you're looking for? If you're looking for documentation for previously released versions of this product, go to the Citrix Knowledge Center. For a complete list of links to all product documentation in the Knowledge Center, go to <http://support.citrix.com/productdocs/>

EdgeSight 5.4

Citrix® EdgeSight™ is a performance and availability management solution for endpoint, XenDesktop, and XenApp systems. EdgeSight monitors applications, devices, sessions, license usage, and the network in real time, allowing users to quickly analyze, resolve, and proactively prevent problems.

In This Section

Under this node, you will find the following resources for EdgeSight:

About EdgeSight	An overview of EdgeSight and its features
New Features for EdgeSight 5.4	New features in this release
Known Issues in EdgeSight 5.4	Known issues in this release
Fixed Issues in EdgeSight 5.4	Fixed issues in this release
System Requirements for EdgeSight 5.4	System requirements for this release
Install and Configure	Installation procedures for all EdgeSight components
Upgrading EdgeSight	Upgrade and uninstallation procedures
Managing EdgeSight	Component and configuration information
Integrating EdgeSight Alerts with Microsoft System Center Operations Manager	How to use EdgeSight with Microsoft System Center Operations Manager
Troubleshooting EdgeSight	Information on troubleshooting license server monitoring and agent log files

Can't find what you're looking for? If you're looking for documentation for previously released versions of this product, go to the Citrix Knowledge Center. For a complete list of links to all product documentation in the Knowledge Center, go to <http://support.citrix.com/productdocs/>

About EdgeSight

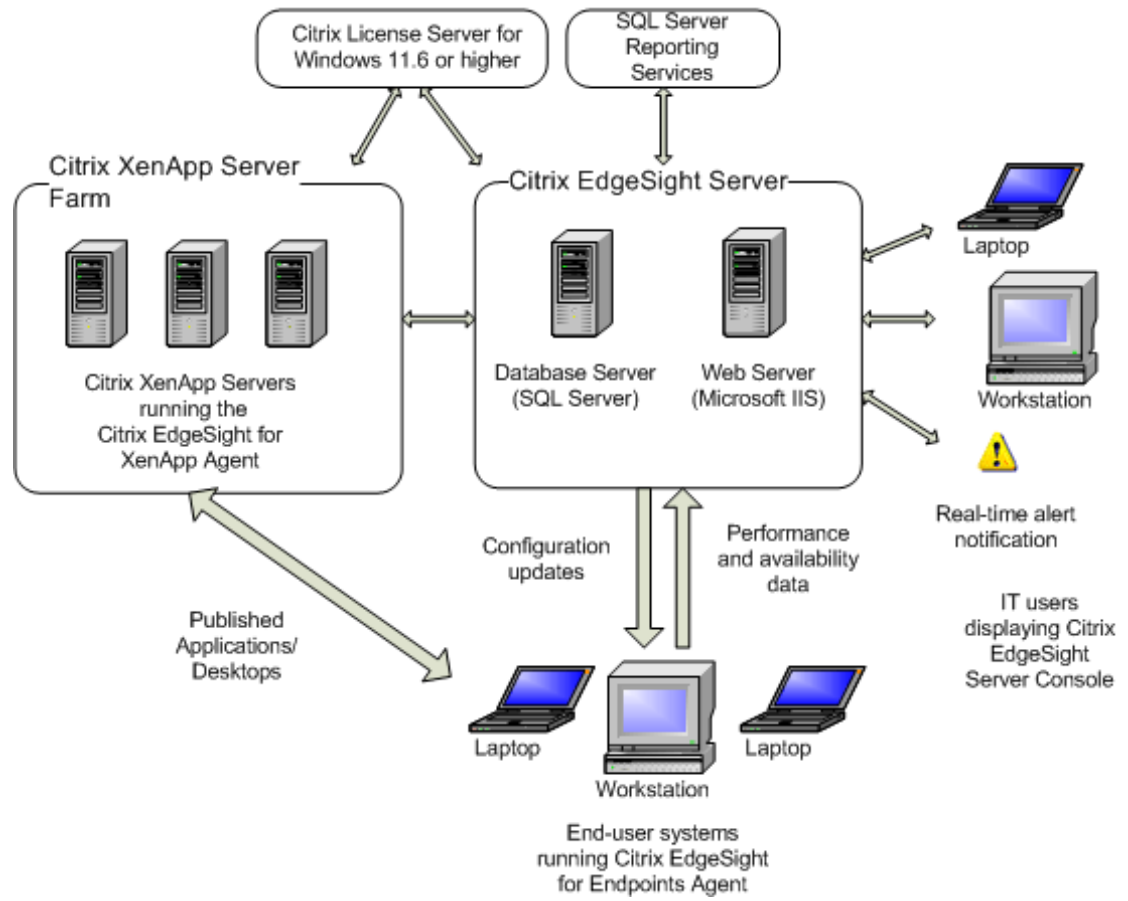
Citrix® EdgeSight™ is a performance and availability management solution for XenDesktop, XenApp and endpoint systems. EdgeSight monitors applications, devices, sessions, license usage, and the network in real time, allowing users to quickly analyze, resolve, and proactively prevent problems. You perform administrative tasks using the Citrix EdgeSight Server Console.

Citrix EdgeSight consists of the following components:

- EdgeSight Agents
- EdgeSight Server
- EdgeSight Server Console
- Citrix License Server

Additional components are required when monitoring virtual desktops, as described in [Installing EdgeSight for Monitoring Virtual Desktops](#). Note that EdgeSight requires the use of SQL Server Reporting Services for the generation of historical reports. See [System Requirements for EdgeSight 5.4](#) for both agent and server system requirements.

The following figure shows the relationship between these components and the systems being monitored:



New Features for EdgeSight 5.4

Contents of this Release

EdgeSight 5.4 consists of EdgeSight Server and EdgeSight Agent components. For the initial release of EdgeSight 5.4, only two components were modified:

- EdgeSight Server (32- and 64-bit versions)
- EdgeSight for XenApp 6 Agent (only available in a 64-bit version, due to the underlying Windows Server 2008 R2 operating system)

No changes were made to the other EdgeSight components, so they remained at their existing version levels. The EdgeSight 5.4 release media therefore included the following components:

- EdgeSight Server 5.4 - NEW
- EdgeSight for XenApp 6 Agent 5.4 - NEW

Note: This agent replaces the EdgeSight for XenApp 6 Agent 5.3, which monitored XenApp 6.0 for Windows Server 2008 R2 systems; the new agent adds support for monitoring XenApp 6.5 systems.

- EdgeSight for XenApp Agent 5.3 Hotfix 4
- EdgeSight for Endpoints Agent 5.3 Hotfix 2
- EdgeSight for Virtual Desktops Agent 5.3 HotFix 2
- EdgeSight Agent Database Server 5.3
- EdgeSight Active Application Monitoring (AAM) 5.3 SP2

Note: Certain older versions of EdgeSight agents can also upload data to an EdgeSight 5.4 Server. For details, refer to the version compatibility matrices in [System Requirements for EdgeSight 5.4](#).

To download the latest hotfixes, go to <http://support.citrix.com> and search for **EdgeSight hotfix**.

New Features

EdgeSight 5.4 includes the following new features:

- Agent support for XenApp 6.5 for Windows Server 2008 R2.
- Support for SQL Server Reporting Services 2008 R2.

- Reporting on user/device license usage in the license trend and usage reports available on the **Track Usage** tab.
- The ability to export a list of user/device licenses currently checked out from a selected license server running Citrix Licensing 11.9. The **User/Device License List** is available on the **Track Usage** tab.
- The addition of advanced EdgeSight Agent properties used to regulate the number and frequency of event log message alerts for each log type (Application, Security, and System).

New and Revised Reports and SQL Views

The **User/Device License List** is the only new report included in this release.

There are no new SQL views, but the vw_lsm_archive_license_statistics (License Server Monitor Archive) SQL view was revised to remove unused fields and add fields related to user/device license data. The following fields were removed:

- license_type
- grace_period
- component_list
- subscription_advantage
- overdraft_protection
- days_to_expire
- perm_license_count

The following fields were added:

- total_user_count
- total_device_count

Use of the revised SQL view requires EdgeSight Server 5.4 and Citrix Licensing 11.9.

Citrix License Server Monitoring

You can use EdgeSight 5.4 to monitor license servers that are running Citrix Licensing 11.9.

Important: If you are upgrading from EdgeSight 5.3 and have been monitoring license servers running earlier versions of Citrix Licensing, you must upgrade to Citrix Licensing 11.9 to monitor those license servers with EdgeSight 5.4.

Known Issues in EdgeSight 5.4

The following is a list of known issues in this release. Read it carefully before installing the product.

Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent

There is a known incompatibility with the McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent.

Workaround: Do not install the agent on devices where this McAfee firewall is running. If McAfee HIPS is required on a computer running the EdgeSight Agent, please contact McAfee support for details on how HIPS can be configured to avoid this issue.

Installation Issues

Important: Before you install this product, make sure you consult [Install and Configure](#).

EdgeSight Agent Should Not Be Installed on Same Machine as the EdgeSight Server

The EdgeSight Agent should not be installed on the same machine hosting the EdgeSight Server. Problems with opening and saving payloads will occur on the server if the agent is subsequently uninstalled. Re-installing the server fixes this problem.

EdgeSight Agent Should Not Be Installed on Same Machine as the EdgeSight Agent Database Server

The EdgeSight Agent should not be installed on the same machine hosting the EdgeSight Agent Database Server due to registry issues. Uninstalling the agent and re-installing the server fixes this problem.

EdgeSight Server Installation Fails If Database Name Contains a Dot (.)

The EdgeSight Server install fails if there is a dot (.) in the database name. See [Installing EdgeSight Server](#) and Microsoft SQL Server documentation for information on valid database naming.

EdgeSight Server Should Be Installed Before the License Administration Console in a Single Machine Installation

If the License Administration Console and EdgeSight Server are installed on the same machine, install the EdgeSight Server before installing the License Administration Console. Installing the License Administration Console before installing the EdgeSight Server will result in the inability to access the EdgeSight Server web site.

Uninstalling EdgeSight Server on Windows Server 2008 When Using Non-Standard IIS Web Port

Attempting to uninstall EdgeSight Server on Windows Server 2008 through Add/Remove Programs when using a nonstandard IIS Web port (for example, port: 94) will fail.

Workaround: Run `setup.exe` and select **Remove**, or change the Web port to the default of 80, uninstall using Add/Remove Programs, then change the port back to the original setting.

Active Application Monitoring Issues

Japanese Character Display Issues

Japanese window title strings are not displayed correctly in Active Application Monitoring controller scripts when used together with XenApp 5.0 and XenApp Plug-in 11.000. If you wish to use this configuration, please update the Plug-in version to 11.100 or higher, by downloading Desktop Receiver - Version 11.100 or higher.

Recording or Editing Scripts to Replay Input of Japanese Characters Not Supported

Active Application Monitoring does not support recording or editing scripts to replay input of Japanese characters. This is a design limitation. For more information, please see <http://support.citrix.com/article/CTX119267>.

Desktop Not Properly Sized When Using ICA Client 11 and Windows 2008

When using the ICA version 11 client to connect to Windows 2008, the display of the desktop is not properly sized. This is a known ICA version 11 client issue and is currently being investigated.

Only ASCII ICA File Names are Supported

Only ICA files with ASCII names should be used for EdgeSight Active Application Monitoring connections. ICA files with non-ASCII character names may prevent users from recording and replaying scripts.

Only ASCII Launcher Names are Supported

Only ASCII Launcher names are supported. If you enter a non-ASCII Launcher name, the Could Not Connect to Launcher message box is displayed.

Fixed Issues in EdgeSight 5.4

Fixed issues

For a list of issues fixed in EdgeSight 5.4, see <http://support.citrix.com/article/CTX124164>.

System Requirements for EdgeSight 5.4

There are separate system requirements for EdgeSight Server and the various types of EdgeSight Agents, plus additional requirements depending on the environment being monitored.

Version Compatibility Matrices

Agents supported by EdgeSight Server 5.4 can monitor the following versions of XenApp:

Agent	XenApp 6.5	XenApp 6.0	XenApp 5.5	XenApp 5.0	XenApp 4.5
EdgeSight for XenApp 6 Agent 5.4 (64-bit only)	x	x			
EdgeSight for XenApp 6 Agent 5.3 (64-bit only)		x			
EdgeSight for XenApp Agent 5.3 (32- and 64-bit versions)			x	x	x

EdgeSight Server 5.4 also supports uploading data collected about system- and session-related performance for instances of XenDesktop:

Agent	XenDesktop 5.5	XenDesktop 5.0	XenDesktop 4.0
EdgeSight for Virtual Desktops Agent 5.3	x	x	x

The following agent can monitor physical endpoint devices and upload the data to EdgeSight Server 5.4:

Agent	Endpoint devices
EdgeSight for Endpoints Agent 5.3	x

Agent Requirements

The system requirements specific to each agent are listed below.

EdgeSight for XenApp agent - for deployment on XenApp systems

XenApp configuration	The target XenApp machine must meet the requirements listed in your XenApp documentation.
Other requirements	The Terminal Services service must be running to properly collect process and network data related to user sessions. (If this service is not running, process and network data cannot be associated with a session and reports dependent on this information show no data.) The session user must be a member of either the Remote Desktop users group or the Administrator users group to collect End User Experience Monitoring (EUEM) data.

EdgeSight for Endpoint agent - for deployment on physical endpoint devices	
OS	Microsoft Windows XP SP2 or higher, Microsoft Windows Server 2003, Microsoft Windows Vista (Business edition or above), Windows 2008, Windows 2008 R2, or Windows 7. Both 32-bit and 64-bit systems are supported on all platforms.
CPU	500 MHz or later recommended
Memory	128 MB of RAM (256 MB recommended)
Disk	100 MB free space (25 MB of disk space for product installation and 75 MB disk space for the database)

EdgeSight for Virtual Desktops agent - to collect system-related and session-related performance data on XenDesktop instances	
OS	Microsoft Windows XP SP2 or higher, Microsoft Windows Server 2003, Microsoft Windows Vista (Business edition or above), Windows 2008, Windows 2008 R2, or Windows 7. Both 32-bit and 64-bit systems are supported on all platforms.
CPU	500 MHz or later recommended
Memory	128 MB of RAM (256 MB recommended)
Disk	30 MB free space

Note: The EdgeSight for Virtual Desktops Agent is not designed to monitor the Desktop Delivery Controller (DDC) in a XenDesktop farm.

The EdgeSight agent installers check the operating system on the target machine. This helps ensure that the correct agent is installed on various devices.

- Attempts to install the EdgeSight for Endpoint agent on any system running a server operating system will result in a warning notifying you that you may be installing the wrong product. You have the option to continue installation. During a silent installation

to a system running a server OS, the install fails unless the ALLOWSERVEROS property is set to 1. A message indicating the cause of installation failure is placed in the install log.

- Attempts to install the EdgeSight for Endpoint agent on a virtual desktop running XenDesktop will result in a message being displayed notifying you that you may be installing the wrong product. You have the option to continue installation. During a silent installation to a system running a XenDesktop, the install fails unless the ALLOWVIRTUAL property is set to 1. A message indicating the cause of installation failure is placed in the install log.
- Any attempt to install the EdgeSight for XenApp agent on a computer not running Terminal Server in Application Mode will fail. (Note that the agent installation does not check to ensure that the Terminal Server is properly licensed.) There is no override.

Server Requirements

The system requirements for the EdgeSight Server are listed below:

Web Server

OS	<p>Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008, or Microsoft Windows Server 2003 SP1 or later. Both 32-bit and 64-bit systems are supported where available.</p> <p>Internet Information Services (IIS) 7.0 for Windows Server 2008. See "IIS 7.0 Components Required on Windows Server 2008 Systems" later in this topic for a list of specific components.</p> <p>Citrix Licensing (This can be installed on a separate system; see "Citrix Licensing Requirements" later in this topic for more information.)</p> <p>Microsoft Message Queuing (MSMQ), Common components only</p> <p>Microsoft .NET Framework 3.5 SP1</p> <p>Note: To support the forwarding of alerts to Microsoft® System Center Operations Manager (SCOM), the SCOM agent must be installed on the EdgeSight Web server. See "Requirements for Forwarding Alerts to System Center Operations Manager" later in this topic for more information.</p> <p>Note the following configuration requirements:</p> <p>Default Web Site running</p> <p>ASP.NET allowed in IIS</p> <p>IWAM and IUSR users active and enabled</p> <p>IIS_WPG group enabled and ASPNET user enabled (if using Windows Server 2003)</p>
CPU	2 gigahertz (GHz) or faster CPU
Memory	2GB of RAM recommended. 512MB of RAM required.
Disk	Minimum 2 GB free space
Database Server	

OS	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008, or Microsoft Windows Server 2003 SP1 or later. Both 32-bit and 64-bit systems are supported where available. The server edition must support SQL Server. See SQL Server Books Online for information on system requirements.
Database	<p>SQL Server 2008 R2 (Standard or better), SQL Server 2008 SP2 (Standard or better), or SQL Server 2005 SP4 (Standard or better). For more information on supported databases, refer to http://support.citrix.com/article/CTX114501.</p> <p>Note that SQL Server 2011 is not supported.</p> <p>Important:</p> <p>Note the following configuration requirements:</p> <p>As of SQL Server 2008, the Reporting Services Role called Manage Shared Schedules no longer exists as a stand-alone role; it is now part of the System Administrator Role. For more information, see Configuring Reporting Services.</p> <p>SQL Server must be configured for case-insensitive collation. Case-sensitive collation is not currently supported for this release.</p> <p>SQL Server should be configured to use Windows Authentication or Mixed-Mode Authentication.</p> <p>Reporting Services is included with SQL Server 2008 R2, SQL Server 2008 and SQL Server 2005. Reporting Services can be installed on a separate machine from the data source.</p> <p>SQL Agent Service running and set to start automatically (if Reporting Services is installed on the machine)</p>
CPU	2 GHz or faster CPU
Memory	2GB of RAM recommended. At least 1 GB of RAM required.
Disk	Minimum 20 GB free space

Agent Database Server

The agent database server is only required if EdgeSight for Virtual Desktops Agents are used to monitor virtual desktops. The server can be installed on a physical or a virtual machine. The EdgeSight Agent Database Server should not be installed on the same machine as the EdgeSight Server. See “Virtual Desktop Monitoring Requirements” later in this topic and [Installing EdgeSight for Monitoring Virtual Desktops](#) for more information.

OS	Windows 2008 R2, Windows Server 2008 or Windows Server 2003 SP1 or later. Microsoft .NET Framework Version 2.0 or later is required.
CPU	2 GHz or faster CPU
Memory	2GB of RAM recommended. At least 1 GB of RAM required.
Disk	Typical disk space usage is generally 70 MB per virtual desktop for the databases on a single disk.

Note: The Web Server (IIS), Database Server (SQL Server), and Reporting Services can be installed on the same machine. We recommend having at least 2 CPUs in such a configuration.

IIS 7.0 Components Required on Windows Server 2008 Systems

Specific IIS 7.0 components are required on a Windows Server 2008 or later system which will be hosting an EdgeSight Server. These components are checked by the bootstrapper program. When configuring IIS 7.0, ensure that the following role services are selected under the Web Server role:

- Static Content
- Default Document
- ASP.NET
- ISAPI Extensions
- ISAPI Filters
- Windows Authentication
- Request Filtering
- The following Management Tools:
 - IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting
 - IIS 6 Management Console

Requirements for Monitoring Session Experience

EdgeSight for XenApp provides highly granular session experience monitoring data collected through XenApp and ICA client instrumentation. This data includes metrics on network bandwidth, ICA round trip time, and client and server startup time. Collection of these metrics depends on the following set of software components:

- Presentation Server 4.5 (or later) or XenApp 5.0 (or later) Enterprise or Platinum Edition
- Appropriate EdgeSight for XenApp Agent running on the Presentation Server or XenApp server
- ICA client version 10 or later

See the [Data Collection by Presentation Server or XenApp Server Version](#) for more information on data collection in relation to software component versions.

Requirements for Forwarding Alerts to System Center Operations Manager

An alert action can be configured to forward EdgeSight alerts generated from EdgeSight for XenApp agents to System Center Operations Manager (SCOM). Currently, SCOM 2007 SP1 and SCOM 2007 R2 are supported. The following software must be installed to enable the forwarding of alerts:

- The following management packs must be imported to the Operations Manager 2007 Server:
 - Citrix Library Management Pack (Citrix.Library.mp)
 - Citrix XenApp Management Pack (Citrix.PresentationServer.mp)
 - Citrix EdgeSight Management Pack (Citrix.EdgeSight.mp, provided on the EdgeSight media)
- The following software must be installed on the XenApp system being monitored:
 - EdgeSight for XenApp Agent
 - Operations Manager Agent
- The following software must be installed on the EdgeSight Server from which alerts will be forwarded:
 - Operations Manager Agent
 - Operations Manager Console or Operations Manager Authoring Console.

Currently, only alerts from EdgeSight for XenApp agents can be forwarded. See "Configuring the Alert Action" under [Installing and Configuring Components](#) for detailed instructions on enabling alert forwarding from EdgeSight to SCOM.

Browser Requirements

EdgeSight Server Console users must have Internet Explorer version 7.0, 8.0, or 9.0 with JavaScript enabled. The following table lists software components that are required on systems from which users access the EdgeSight Server Console:

Software	Used to...
Microsoft Excel (as included with Microsoft Office 2003 or Microsoft Office 2007). Note that Microsoft Excel 2010 is not supported.	Display remote reports from the EdgeSight Server Console. Note: Ensure that Visual Basic for Applications is selected from Office Shared Features when customizing the Microsoft Excel installation.
Adobe Flash Player 10.0 or later	Display Flash-based reports and consoles. (Not currently available on 64-bit browsers.) If you do not have Flash Player installed on your system, you will be prompted to download the software.
Adobe Acrobat Reader	Display reports exported in a PDF format.

Operating System Language Support

Operating system languages must match in configurations where the EdgeSight database and Web server are installed on separate machines.

Citrix Licensing Requirements

EdgeSight 5.4 requires licenses allocated from Citrix Licensing 11.6 or later. If the Citrix License Server is not installed and running, license information cannot be obtained, and EdgeSight Agents are not allowed to upload data to the EdgeSight Server. You will receive instructions by email for downloading the EdgeSight license code. For documentation on licensing, including system requirements and installation instructions, see the [Citrix Licensing documentation](#).

Install the license server from the EdgeSight media (**EdgeSight Component Installers > Install Citrix Licensing**). The license server can be installed on the same system as the EdgeSight Web server, or it can be installed on another system, as long as it is accessible by the Web server. The license server can be shared by multiple EdgeSight servers.

Important: If you are installing the License Administration Console and EdgeSight Server on the same machine, install EdgeSight Server first. Installing the License Administration Console first precludes access to the EdgeSight Server web site. Also, if there is a firewall between the license server and the computers running EdgeSight components, you must specify a static Citrix Vendor Daemon Port number on the license server.

When installing the license server, accept the defaults provided by the MSI file for the destination folder and the license file location. When selecting features, you can choose

whether to select the License Administration Console; this feature is not required, but may be useful in managing your licenses.

Additional Requirements for Monitoring Citrix License Servers

Although you can still obtain Agent licenses from earlier versions of Citrix Licensing (as explained above in the section on Citrix Licensing Requirements), the EdgeSight 5.4 License Server Monitoring feature only works with license servers that are running Citrix Licensing 11.9. Attempting to monitor an incompatible license server will generate an error during data polling.

Tip:

- To monitor a license server associated with XenApp 6.5 for Windows Server 2008 R2 systems, you must run Citrix Licensing 11.9 on the license server and use EdgeSight 5.4.
- If you choose to remain with an earlier version of XenApp but want to use the new license monitoring features available in EdgeSight 5.4, you must upgrade your license server to Citrix Licensing 11.9.
- If you have been monitoring earlier versions of Citrix Licensing using EdgeSight 5.3 and you want to monitor those license servers using EdgeSight 5.4, you must upgrade to Citrix Licensing 11.9.
- If you want to continue to monitor earlier versions of Citrix Licensing (11.5, 11.6, or 11.6.1), you should configure a separate server running EdgeSight 5.3.

The License Server Monitoring feature is not dependent on the EdgeSight agents, because license servers are polled directly by EdgeSight Server. License servers must be explicitly identified using the EdgeSight Server Console before they are monitored for license type, usage, and availability.

Active Application Monitoring Requirements

The system requirements for systems running the EdgeSight Active Application Monitoring Controller and Launcher are listed in the following table.

Controller and Launcher Requirements

OS	<p>Controller</p> <p>Microsoft Windows Vista, Microsoft Windows XP, Microsoft Windows 7, Microsoft Windows Server 2003, Microsoft Windows Server 2008, and Microsoft Windows Server 2008 R2 (32-bit and 64-bit systems on all operating systems)</p> <p>Launcher</p> <p>Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows Server 2003 (32-bit systems only), Microsoft Windows Server 2008, and Microsoft Windows Server 2008 R2 (32-bit and 64-bit systems on all operating systems except as noted)</p> <p>ICA Client Version 10 or higher</p> <p>Citrix Presentation Server 4.0 or higher, Citrix XenApp 5.0 or 6.0</p> <p>.NET Framework 2.0 or later is required for all Launchers and Controllers that will be establishing connections using the Web Interface.</p> <p>Visual J# Version 2.0 (if using XML Interface Connector)</p> <p>EdgeSight for XenApp Agent, Advanced Mode, must be installed on the server under test. If a Basic mode agent is installed, application response alerts will not be generated and no data will be displayed in application response reports.</p>
CPU	2 gigahertz (GHz) or faster CPU
Memory	1 gigabyte (GB) of RAM
Disk	Minimum 200 megabytes (MB) of free space

Virtual Desktop Monitoring Requirements

You can use EdgeSight to monitor virtual desktops. The following tables list software components used in such an environment. (As with any EdgeSight deployment, you will also need SQL Server Reporting Services and Citrix Licensing, as specified in this document.) For instructions on installing the EdgeSight components in a virtual desktop environment, see [Installing EdgeSight for Monitoring Virtual Desktops](#).

In a production environment, the EdgeSight Agent Database Server supports up to 40 EdgeSight for Virtual Desktops agents. If over 40 EdgeSight for Virtual Desktops agents are to be deployed, install additional Agent Database Servers to handle the additional agent

System Requirements

data. Alternatively, you can use locally attached, persistent storage. See <http://support.citrix.com/article/CTX126414> for deployment considerations.

When monitoring virtual desktops running XenDesktop, the following software components must be in place:

Software Component	For more installation information...
XenDesktop 4.0 or later	XenDesktop 4 System Requirements XenDesktop 5 System Requirements XenDesktop 4 (installation information is under "XenDesktop 4 Service Pack 1" and "Administering XenDesktop") Installing and Setting up XenDesktop 5
EdgeSight Server 5.3 or later	Installing EdgeSight Server
EdgeSight for Virtual Desktops Agent 5.3 or later	Installing EdgeSight for Monitoring Virtual Desktops
EdgeSight Agent Database Server 5.3 or later	Installing EdgeSight for Monitoring Virtual Desktops

Install and Configure

Preparing to Install Citrix EdgeSight

Citrix® EdgeSight™ software includes the following components:

- EdgeSight Server – Displays performance data for monitored devices.
- EdgeSight for XenApp Agent – Monitors the performance of XenApp and Presentation Server systems. Multiple versions of the agent are provided to accommodate different XenApp versions.
- EdgeSight for Endpoints Agent – Monitors the performance of physical clients.
- EdgeSight for Virtual Desktops Agent – Monitors the performance of instances of XenDesktop 4.0 or later. This agent enables the following features:
 - Collection of ICA channel data including XenDesktop multi-media counters
 - Collection of End User Experience metrics
 - Alerting on XenDesktop session performance
- EdgeSight Agent Database Server – Stores performance data for agents monitoring virtual desktops.
- EdgeSight Active Application Monitoring (AAM) Components – Performs automated testing to monitor the end user experience of applications in XenApp and Presentation Server environments.

Citrix EdgeSight software is installed using Windows Installer (MSI) files. The EdgeSight Server MSI files are invoked using a bootstrapper program (setup.exe). The following table lists the MSI files by EdgeSight component. Separate MSI files are provided for 32-bit and 64-bit systems for EdgeSight Server and EdgeSight Agents.

EdgeSight Component	MSI Name
EdgeSight Server (32-bit systems)	EdgeSightServer.msi
EdgeSight Server (64-bit systems)	EdgeSightServerx64.msi
EdgeSight for XenApp Agent for XenApp 6 (64-bit only, due to underlying operating system) Note: Use this agent for monitoring XenApp 6 and XenApp 6.5 for Windows Server 2008 R2 systems.	EdgeSightXA6Agentx64.msi
EdgeSight for XenApp Agent (32-bit systems)	EdgeSightXAAgent.msi

EdgeSight for XenApp Agent (64-bit systems)	EdgeSightXAAgentx64.msi
EdgeSight for Endpoints Agent (32-bit systems)	EdgeSightEPAgent.msi
EdgeSight for Endpoints Agent (64-bit systems)	EdgeSightEPAgentx64.msi
EdgeSight for Virtual Desktops Agent (32-bit systems)	EdgeSightVDAAgent.msi
EdgeSight for Virtual Desktops Agent (64-bit systems)	EdgeSightVDAAgentx64.msi
EdgeSight Agent Database Server	EdgeSightAgentDBS.msi
EdgeSight Active Application Monitoring components (Controller, Launcher, and Web Interface)	EdgeSight Active Application Monitoring.msi
Citrix License Server	CTX_Licensing.msi

Note: Do not modify the base MSI files. Modifying the base MSI files can interfere with support efforts in case of installation issues. You can customize the installation by specifying options and properties on the command line or by creating a transform.

Server Installation Overview

Use setup.exe to install an EdgeSight Web server and database server. After you install and configure the server components, deploy the applicable EdgeSight Agent to XenApp Servers, end-user systems, and virtual desktops. In addition to the software listed in “Server Requirements” in [System Requirements](#), EdgeSight Server requires the following software. It is highly recommended that you install the following software before installing EdgeSight Server software.

- **Microsoft SQL Server Reporting Services**—required for the generation of historical reports. Reporting Services must be in place before reports can be generated and displayed. For information on configuring Reporting Services for use with EdgeSight software, see [Configuring Reporting Services](#).
- **Citrix Licensing**—used to supply a license authorizing the agent to upload data to a Citrix EdgeSight Server. The license server can be installed anywhere on the network and can be shared by multiple EdgeSight servers. The license server and EdgeSight license files must be in place before data can be uploaded to the server. A Citrix License Server MSI is included with the EdgeSight media for your convenience. For more information and supported versions, see “Citrix Licensing Requirements” in [System Requirements](#).

When planning your installation, the required server components can be installed on separate physical machines. (The Web server can be installed on the same machine as the database server, but the machine should have at least two processors.) In all cases, ensure that the machines have sufficient memory and processor capabilities (as described in “Server Requirements” in [System Requirements](#)) and that the machines are in the same domain.

The MSI file installs server files for both EdgeSight for XenApp and EdgeSight for Endpoints. Both products use the same underlying server technologies. You can enable or disable agent support for either product after installation.

Note: EdgeSight Server should not be installed on the same system as XenApp in a production environment, but this can be done to support a proof of concept environment.

Agent Deployment and Installation Overview

Use the applicable EdgeSight Agents MSI file to install EdgeSight agents on target machines. Separate MSI files are provided for each type of agent (EdgeSight for XenApp, EdgeSight for Virtual Desktops, and EdgeSight for Endpoints), for each target system architecture (32-bit and 64-bit), and for XenApp versions (Presentation Server / XenApp 5 and XenApp 6). The EdgeSight for XenApp Agent MSI file provides both the Basic and Advanced versions of the agent. You can deploy agents to end-user systems or XenApp Servers in your enterprise using several methods:

- Direct command-line or GUI-based installations using the MSI file.
- Define an Active Directory Group Policy Object for software distribution of the MSI file. Note that GPO push to users is supported.
- Perform a System Management Server (SMS) issuance of the MSI file.

If you are installing the EdgeSight for Endpoints agent or the EdgeSight for Virtual Desktops agent on virtual desktops, additional software components and installation tasks are required, as described in [Installing EdgeSight for Monitoring Virtual Desktops](#). Discuss your software deployment environment with your Sales Representative; they can assist you in implementing an effective means of deploying the agent.

Active Application Monitoring Installation Overview

EdgeSight Active Application Monitoring is an automated performance testing tool that periodically samples critical application transactions to monitor the availability and responsiveness of virtualized applications, providing insight into application performance and end-user experience.

EdgeSight Active Application Monitoring software includes the following components:

- Citrix EdgeSight Controller—used to record and create virtual user scripts and define tests. When the test is ready for playback, the Controller instructs the Launchers to run the test for a specific period of time.
- Citrix EdgeSight Launcher—receives commands from the Controller and generates virtual user ICA sessions on the target Presentation Servers and XenApp servers. The number of Launchers required will vary based on the target virtual user load.
- Web Interface Connector—allows users to connect to applications made available through the XML Service. This feature requires the Visual J# Version 2.0 Redistributable Package available from Microsoft.

Launchers are installed on clients of the Servers that will be under test. They can be installed on systems with the Controller and as stand-alone launchers. See [Installing EdgeSight Active Application Monitoring Software](#) for installation procedures for these components.

Pre-Installation Considerations

Software running in your environment may need to be configured to allow Citrix EdgeSight software to operate properly. Review the following considerations and related actions and determine if they apply to your environment.

Agent

- **Proxy Servers and Settings**—If the EdgeSight Agent will communicate with the EdgeSight Server through a proxy server, ensure that you have the proxy server IP address, port number, and credentials required prior to installing EdgeSight Agent. See [Installing EdgeSight Agents](#) for instructions on specifying proxy server information during agent installation.
- **Firewalls**—If firewall software is resident on machines on which EdgeSight Agents will be installed, the listen port on the client machine (port 9035) must be open. This is the port on which the agent listens for remote connections from the browser displaying the EdgeSight console. There is an option during agent installation to automatically set a Windows Firewall exception for the listen port if the firewall is running (enabled or disabled). See [Installing an Agent Using the User Interface](#) for instructions on specifying the listen port number. Also see “Configuring Firewalls” in [Configuring Third Party Software](#) for information relating to personal firewalls.
- **Virus scanning software**—If your environment uses virus scanning software, script blocking features must be disabled to allow the EdgeSight Agent to run scripts. Also, exclude agent data files from being scanned. See “Configuring Antivirus Software” in [Configuring Third Party Software](#) for detailed information on which files should be excluded from scans.

Server

- **Virus scanning software**—If your environment uses virus scanning software, script blocking features must be disabled to allow EdgeSight Server to run scripts. Also, exclude the server database from being scanned. See “Configuring Antivirus Software” in [Configuring Third Party Software](#) for detailed information on which files should be excluded from scans.
- **IIS Security Lockdown template**—Any IIS Security Lockdown templates must allow the IIS components listed in “Server Requirements” in [System Requirements](#) to run. Adjust the template as required.
- **Group Policy**—Ensure that Group Policies do not prohibit any of the required software components from running on your EdgeSight Server. Also, ensure that policy changes that would prohibit software components from running are not scheduled for deployment after the installation is complete.
- **SQL Server 2005 Password Policy**—SQL Server 2005 includes an option to enforce Windows password policy. This option is enabled by default and will cause an error if the passwords supplied for accounts during installation do not meet the necessary

strength requirements. If an error occurs containing the text, “Password validation failed. The password does not meet Windows policy requirements because it is not complex enough,” then double check your password requirements, reattempt installation, and supply appropriately complex passwords.

- **SSL Certificate**—If you choose to enable SSL for use on the Citrix EdgeSight Web server, you must either use an SSL certificate from a recognized certificate authority or a correctly generated and installed certificate from Microsoft Certificate Server to allow proper software operation. For detailed information, see [How to Configure EdgeSight to use SSL with Microsoft Certificate Services](#). SSL certificates which do not meet these criteria do not allow remote pages to be displayed or remote scripts to be run. Attempts to perform these actions without a valid certificate result in an error message.

Citrix Systems recommends the use of SSL (HTTPS mode) when accessing the EdgeSight Server Console. The use of HTTP mode is not recommended. Failure to use SSL can increase the risk of security breaches including, but not limited to, disclosure of sensitive information including passwords and session cookies, potential compromise of the administrator account, session hijacking, and arbitrary execution of commands.

If it is not possible to get a standard CA-signed certificate for each server, the following approach may be taken. Install an organization-wide CA (CA-Org) which has a certificate of itself. This CA can now sign the public keys for all servers in the organization. When any client (browser) tries to connect to any of these servers over HTTPS, it will get a server certificate which is signed by CA-Org. For the browsers to be able to accept the server certificate and work seamlessly without giving any warnings, it is required that the certificate of CA-Org is accepted by all browsers. Either the certificate of CA-Org is signed by a standard CA like Verisign or GeoTrust which the browsers accept by default, or the self-signed certificate of CA-Org is pre-installed on all the browsers in the organization. In both the cases, the communication would be secure as long as the private key of CA-Org is not compromised.

- **SMTP Server**—During installation, you must specify an SMTP server. It is important that a valid SMTP server name is used. EdgeSight Server uses the SMTP server for many operations, including the distribution of alert notifications, server error conditions, and new user passwords.

Installing EdgeSight Server

The server installation is launched using the setup.exe bootstrapper. The installation will fail if the server MSI file is invoked directly.

The preferred method of installing EdgeSight Server is to use the bootstrapper and perform the installation using the Citrix EdgeSight Installer user interface. This method offers typical and custom installation options. A typical installation offers only the minimum set of properties required for installation. A custom installation offers the same set of public properties as a command-line installation.

If required, you can perform a command-line installation using the msiexec command. You must specify public properties to define installation settings. Review [Installing EdgeSight Server Using the Command Line](#) for a description of installation properties.

If you are upgrading, see [Upgrading EdgeSight](#) for more information.

If you are monitoring endpoint devices, download EdgeSight for Endpoints license files (CES_*.lic), then manually place them in the MyFiles folder of the license server directory, for example: %ProgramFiles%\Citrix\Licensing\MyFiles. These files will need to be in place prior to running the post-installation wizard.

Prerequisite Checking

The bootstrapper performs checks for the following software prerequisites and system characteristics. The conditions checked can be required or recommended. If any of the required conditions is not met, the installation stops. Correct the condition and restart the installation. Recommended conditions are flagged with a warning, but installation can continue at the discretion of the installer.

Condition	Required
.NET Framework 3.5 SP1	Yes
Windows Server 2003 or Windows Server 2008	Yes
Internet Information Services (IIS) 6.0 or later. See “IIS 7.0 Components Required on Windows Server 2008 Systems” in System Requirements for information specific to IIS 7.0 and Windows Server 2008.	Yes
Microsoft Message Queuing (MSMQ). The MSMQ service must be running.	Yes
SQL Server 2005 SP1 or later (Standard or better). This can be on a different machine from where the installation is being run.	Yes

<p>512 megabytes (MB) of RAM</p> <p>Note that 2GB is recommended.</p>	<p>No. Installation can continue, but performance may be affected.</p>
<p>SSL certificate from a recognized certificate authority. See Install and Configure for more information on SSL certificate considerations.</p>	<p>No, installation can continue, but security may be compromised.</p>

Note that some requirements for full operation, such as Citrix Licensing and SQL Server Reporting Services, are not checked by the bootstrapper.

Installing EdgeSight Server Using the User Interface

Before performing an EdgeSight Server installation, set up a “run as” account for EdgeSight. You will need to supply the account username and password during server installation. Specify the account using the computer name and username (*computername\username*) or the domain name and username (*domainname\username*). Do not use a fully qualified domain name (FQDN), as this will result in an installer error.

Note that not all public installation properties are exposed when performing a typical installation using the user interface. Properties not explicitly set from the user interface are set to their default value if one exists. However, performing a custom installation will expose all available properties. The following procedure is based on a custom installation. To install a server using the user interface:

1. Insert the media or run Autorun.
2. Select **EdgeSight Server** to display the Choose Language dialog.
3. Select the language for the installation and click **Continue** to display the Welcome screen.
4. Click **Next** to continue to display the Select Features screen.
5. Select the applicable radio button for the EdgeSight Server components to be installed. You can install a Web server and database, or just a database. In both cases, if there is an existing database, it will be upgraded as necessary. Click **Next** to continue to display the Prerequisite Check screen.
6. A check for minimum requirements is performed and the result of the check is displayed. If minimum requirements are not met, the installation is stopped and you are notified of missing components. If minimum requirements are met, but limitations are present due to the configuration of the target system, warnings are displayed. (Examples of warning conditions are the not meeting minimum memory requirements.) You can continue the installation even though warnings have been issued. Click **Next** to display the End-User License Agreement screen.
7. After reading the license, select the **I accept** radio button and click **Next** to display the Choose Setup Type screen.
8. Select the applicable radio button for the type of setup to be performed (Typical or Custom). In this case, choose the **Custom** radio button and click **Next** to display the Database Server screen.
9. Select an existing server name from the list or enter a server name. The name of the machine on which you are running the installer is preloaded into the entry field. You can also enter a named instance in this field (*servername\instancename*).
10. Select an authentication method. The method you choose is partially determined by the accounts set up when SQL Server was installed. (Note that you must have administrative

privileges on the database server.) Click the **Test Connect** button to test the connection to the SQL Server. Click **Next** to display the next Database Information page.

11. Select the **Install a new EdgeSight database** radio button to create a new database. (If you were performing an upgrade, you would select the applicable radio button and choose an existing database from the list.)
12. Enter a name for the new database and click **Next** to display the Database User Information screen.

Database names must be unique within an instance of SQL Server and comply with the rules for identifiers. Also, the database name can not contain hyphens, the pipe character (|), single quotes, a period (.), or spaces.

For information on identifiers, see SQL Server Books Online for your version of SQL Server.

13. Enter and confirm the account username and password that the Web server uses when connecting to the database. If you are performing the installation using local machine accounts, enter the computer name and username (*computername\username*). If you are performing the installation using domain accounts, enter the domain name and username (*domainname\username*). Do not supply a fully qualified domain name, as this will result in an installer error.
14. Click **Validate** to test the user credentials. After the credentials have been successfully validated, click **Next** to display the Database Properties screen.
15. Configure the database properties as follows:

- **File Group Size**—Accept the default file size or enter a new file size. Each of the eight files in the file group is created using the specified size. The default value is sufficient space for most installations. A smaller size may be selected for pilot installations.
- **Log File Size**— Accept the default log file initial size or enter a new file size. The default value is sufficient space for most installations.
- **Recovery Model Options**—Select a database recovery model (Simple, Bulk-logged, or Full) from the drop-down menu. The default recovery model is Simple. If the recovery model is changed to Full, ensure that a database backup strategy is in place to effectively manage database size. See SQL Server Books Online for more information on recovery models.

Note: The installer uses the default file group and log file creations as configured in the SQL Server installations. A SQL Server administrator can change the location of the file groups and log files, but the SQL Server service must be restarted before the new locations will take effect.

16. Click **Next** to display the Server Location screen.
17. Review the default values for the program files root and the data files path. You can accept the default values or click the **Browse** button to select a different location for the files. To display information about space availability on all system drives, click the **Disk Usage** button. When you have specified server file locations, click **Next** to display the Ready to Install screen.

18. Click **Install** to begin the installation. (If you need to review or change any settings before installing, use the **Back** button to return to the configuration screens.) Installation status is displayed while the installation is being performed. When the installation is finished, the Complete screen is displayed.
19. The checkbox indicating you want to go to the EdgeSight Server Website (<http://servername:port/edgesight/app/suilogin.aspx>) is checked by default. You must go to the Website to perform initial configuration tasks, as described in [Running the Post-Installation Setup Wizard](#). (If you want to perform initial configuration at a later time, deselect the checkbox. However, it is recommended that you complete initial configuration directly after completing the installation.) Click **Finish** to exit the installer.

Note: You will need to communicate with the license server during the initial configuration procedure. If you have not installed the license server, deselect the checkbox, close the installer, install the license server, and then log into the Web site.

Installing EdgeSight Server Using the Command Line

The MSI file uses public properties to specify custom install settings. You can edit public properties using the following methods:

- Run the installer user interface (if the property is exposed). A log file is not created when the user interface is used for installation.
- Create a transform file using a tool such as Orca. For more information on using Orca with MSI files, see <http://support.microsoft.com/kb/255905>.
- Specify key/value pairs on the command line. This method allows you to control the full range of installation options, including specifying a log file, as well as being able to specify public properties. The syntax for key/value pairs is *KEY=value*.

See your MSI documentation for syntax rules for property values. The following table lists the public properties available when installing the Citrix EdgeSight Server. You only need to specify properties with default values if you want to specify a value other than the default. Also, whether some properties are specified depends on what other properties are being specified. For example, if Windows authentication is not enabled using the `WINDOWS_AUTH` property, the `DBUSERNAME` and `DBPASSWORD` properties must be defined.

Note: Although additional properties are exposed when you examine the MSI file, only the public properties listed in the following table should be explicitly specified.

Property Name	Description
<code>PREREQUISITES_PASSED</code>	If this property is specified with any value, the bootstrapper is bypassed and you are allowed to perform a command-line installation of the server.
<code>DATABASEOPTIONS</code>	Specifies whether to install a new Citrix EdgeSight database or upgrade an existing database. Valid values are <code>new</code> or <code>upgrade</code> ; the default value is <code>new</code> .
<code>DATABASESERVER</code>	The name of the server running an existing Citrix EdgeSight database. It is not necessary to specify a value when running the database locally.
<code>DBUSERNAME</code>	The username for the SA user. It is not necessary to specify a value if Windows authentication is enabled (<code>WINDOWS_AUTH=1</code>).
<code>DBPASSWORD</code>	The password for the SA user. It is not necessary to specify a value if Windows authentication is enabled (<code>WINDOWS_AUTH=1</code>).

WINDOWS_AUTH	<p>Specifies whether to use Windows authentication. Valid values are 1 (use Windows authentication) or 0 (do not use Windows authentication); the default value is 1.</p> <p>Note: If Windows authentication is not used, the DBUSERNAME and DBPASSWORD properties must be defined.</p>
DBNAME	<p>The name of the Citrix EdgeSight database that will be created during installation. Database names must be unique within an instance of SQL Server and comply with the rules for identifiers. Also, the database name can not contain the pipe character (), single quotes, a period (.), a hyphen (-), or spaces. For information on identifiers, see SQL Server Books Online for the your version of SQL Server. The default value is EdgeSight.</p>
ACCOUNTNAME	<p>The account name for the EdgeSight “run as” account. Specify the account using the computer name and username (<i>computername\username</i>) or the domain name and username (<i>domainname\username</i>). Do not use an FQDN.</p>
ACCOUNTPASSWORD	<p>The password for the EdgeSight “run as” account.</p>
DATAFILESIZE	<p>Specifies the initial size in megabytes of a data file. Each of the eight files in the file group is created using the specified size. The default value is 500 and is sufficient for most installations.</p>
LOGFILESIZE	<p>Specifies the initial size in megabytes of the log file. The default value is 500 and is sufficient for most installations.</p>
RECOVERYMODEL	<p>Specifies the database recovery model. Valid values are FULL, SIMPLE, and BULK_LOGGED; the default value is SIMPLE.</p>
DATADIR	<p>EdgeSight Server uses temporary files for storing data uploads from agents, including crash reports. The default directory is %ProgramFiles%\Citrix\System Monitoring\Server\EdgeSight\Data. Because there may be significant file growth in this directory, it may be desirable to locate this directory on a separate drive or partition.</p> <p>Note: The data directory cannot be on a mapped drive.</p>
EDGEDIR	<p>Contains the web pages, scripts, .Net components and other components that make up the EdgeSight Server Web site. The default value is %ProgramFiles%\Citrix\System Monitoring\.</p>
INSTALLOPTIONS	<p>Specifies which components are to be installed. Set the value to <i>full</i> to install the database, Web server, and script handler components. Set the value to <i>dbonly</i> to install only the database component.</p>

Use the msixec command to install the server using the command-line interface. Public properties are specified as *KEY=value* pairs. Note that path names must be enclosed in quotes. The following is a sample msixec command line:

```
Msixec /i EdgeSightServer.msi /l*v logfile.log /qn
PREREQUISITES_PASSED=1 WINDOWS_AUTH=1
```

```
ACCOUNTNAME=mydomain\myaccount ACCOUNTPASSWORD=mypass  
DBNAME=EdgeSight50  
DATADIR="D:\Citrix\System Monitoring\Data"
```

The `/i` flag is used to specify the package being installed. The `/l*v` flag is used to specify the installation log file name. (Capturing a verbose installation log is strongly recommended.) Use the `/qn` (quiet) flag to install an agent with no user interaction. For a complete list of standard MSI command-line arguments, open a Command Prompt window and type `msiexec /h` to invoke help, or refer to *The Command-Line Options for the Microsoft Windows Installer Tool Msiexec.exe* at <http://support.microsoft.com/kb/314881>.

Running the Post-Installation Setup Wizard

After you have completed the Citrix EdgeSight Server installation, you must use the Citrix EdgeSight Post-Installation Setup Wizard to perform initial server configuration. The wizard is displayed the first time you log into the EdgeSight Server Web site (<http://servername:port/edgesight/app/suilogin.aspx>). The post-installation wizard helps you perform the following tasks:

- Create a company. A company is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies.
- Create the Superuser account. This account has access to all companies hosted on the server and can create other users.
- Configure email settings. This information is used on notification emails generated by the server.
- Configure agent support.
- Configure licensing if EdgeSight for Endpoint agent support is enabled.

To configure your Citrix EdgeSight Server:

1. Review the tasks you will perform and ensure that you have the information at hand to specify the settings listed above. Click **Next** to display the Create an Initial Company page.
2. Enter a name for the company for which data will be displayed on the Web site.
3. Select a time zone from the drop-down menu to be used by the server when displaying the time and triggering jobs. There is a single time zone for each company defined on a Citrix EdgeSight Server. All data for that company is aggregated based on the day boundary for that time zone. This ensures greater data consistency when agent machines are in a number of different time zones.
4. Select the default display language for new user accounts from the drop-down menu. Click **Next** to display the Create the Superuser Account page.
5. Enter login information for the Superuser account (a universal login ID to be used by the Citrix EdgeSight administrators). This login enables administrators to access data from all companies and perform server administrative tasks. The Superuser account cannot be deleted. Enter a first and last name, a login ID in the form of an email address, and a password. You must confirm the password. Click **Next** to display the Configure Email Settings page.
6. Enter the name of the SMTP server used to route email. The SMTP server can be running locally or remotely.

7. Enter the email address for the person or group who should be notified of important events occurring on the Web site. In most cases, this person is the Citrix EdgeSight Administrator.
8. Enter a display name and email address to be used when email is generated by the Web site. (Once the Web server is installed, you use the EdgeSight Server Console to determine additional criteria for email notifications.) Click **Next** to display the Configure Agent Support and Licensing page.
9. Select which types of agents, if any, to display on the server from the support drop-down menus. For example, if the EdgeSight Server will only be used to monitor XenApp systems, disabling display support for the other types of agents can provide a more streamlined interface. Similarly, if the EdgeSight Server will only be used for license server monitoring, you can disable support for all agents. EdgeSight provides the following types of agents:

EdgeSight for XenApp, Basic—Basic agents require only that you have a XenApp Enterprise license available on your Citrix License Server.

EdgeSight for XenApp, Advanced—Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix License Server.

EdgeSight for Endpoints—Endpoint agents provide monitoring and data collection for endpoint devices.

EdgeSight for XenDesktop—EdgeSight for Virtual Desktops agents provide monitoring and data collection for XenDesktop devices.

Note: This setting only determines whether reports and administrative pages are displayed on the console; the data continues to be collected, uploaded, and stored even if you have disabled display support. You can change the agent display support at any time after installation using the EdgeSight Server Console.

10. Enter the license server name and port number used for communication with the license server which will supply EdgeSight for Endpoints Agent licenses. The license server can be installed on the machine hosting the EdgeSight Web server, or can be installed on another machine as long as it is accessible via the network. (EdgeSight for XenApp Agents obtain their licenses directly from the license server without intervention from EdgeSight Server. They use the license server specified in their agent configuration. See [Managing Licenses](#) for more information on licensing.)
11. This step is optional. After entering the license server name and port, click the **Test License Server** button to ensure that you can connect to the specified license server and that EdgeSight licenses are found. If the test is successful, a success message is displayed, along with the type and number of EdgeSight licenses installed. The test can fail because the license server is not accessible, or because the license server is not the correct version. Verify the license server name and port, or upgrade the license server and retry the test. You may also want to try using the IP address or FQDN of the license server.
12. Click **Next** to display the Review Citrix EdgeSight Server Settings page.
13. Review the selected configuration settings. Use the **Back** button to return to previous pages and adjust settings. When you are satisfied with the settings, return to the review screen and click **Finish** to save the configuration. The Citrix EdgeSight login

page is displayed if the checkbox for this option is selected.

Installing EdgeSight Agents

In most production environments, the agent is deployed and installed as described in “Agent Deployment and Installation Overview” in [Install and Configure](#). You can also perform an agent installation on a single client system. You may want to use this method during evaluation or when deploying and installing small numbers of clients.

If you are deploying agents for monitoring virtual desktops, see [Installing EdgeSight for Monitoring Virtual Desktops](#) for information specific to that environment.

Note: Whatever deployment and installation methods you choose, you must have administrator privileges on the target machines.

Agent Mode

The EdgeSight for XenApp Agent has two modes of operation, Basic and Advanced:

- Basic agents require only that you have a XenApp Enterprise license available on your Citrix License Server.
- Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix License Server.

When an EdgeSight for XenApp Agent is installed on a XenApp or Presentation Server machine, the agent mode enabled by default depends on the version and edition of XenApp or Presentation Server. The following table shows the default agent mode by XenApp and Presentation Server version and edition. The table also shows whether the **Mode** tab is displayed on the Citrix System Monitoring Agent control panel applet.

XenApp or Presentation Server Version	XenApp or Presentation Server Edition	Default Agent Mode	Mode Tab Available
6.5	Platinum	Advanced	No
6.5	Enterprise	Basic	Yes
6.0	Platinum	Advanced	No
6.0	Enterprise	Basic	Yes
5.0	Platinum	Advanced	No
5.0	Enterprise	Basic	Yes
4.5	Platinum	Advanced	No
4.5	Advanced/Standard	Advanced	No

4.5	Enterprise	Basic	Yes
4.0	Platinum	Advanced	No
4.0	Advanced/Standard	Advanced	No
4.0	Enterprise	Basic	Yes

Software Configuration Tasks

You may need to change the configuration of some software, such as antivirus software or personal firewalls, on machines which will run the EdgeSight Agent to ensure proper operation. You can perform these configuration tasks before or after installing the EdgeSight Agent. For more information, see [Configuring Third Party Software](#).

Antivirus Configuration Checking

Due to the manner in which buffer overflow protection was implemented in McAfee VirusScan 8 or 8i with Patch 10, this feature may conflict with the operation of the EdgeSight Agent. (In later versions of McAfee VirusScan, this feature was implemented differently and does not conflict with EdgeSight Agent operation.) The EdgeSight Agent installer checks for McAfee 8 or 8i with Patch 10 or below on the target machine. If the EntApi.dll file is present with version 8.0.0.277 and below, the installation exits with an error. The check is performed on both full UI and unattended installations. In a command-line installation, the check can be omitted from the installation process by specifying the `OVERRIDE_COMPCHECK` property with a value of 1.

Note: The `OVERRIDE_COMPCHECK` property should only be used if you disable the McAfee buffer overflow protection feature as described under "Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent" in the [Known Issues in EdgeSight 5.4](#).

Installing an Agent Using the User Interface

Note that not all public installation properties are exposed when installing using the user interface. Properties not explicitly set from the user interface are set to their default value if one exists. To install an agent using the user interface:

1. Insert the media.
2. Select **EdgeSight Agent Installers**.
3. Select the agent type to be installed to display the Welcome screen.
4. Click **Next** to display the License Agreement screen.
5. After reading the license, select the **I accept** radio button and click **Next** to display the Company Information screen.
6. Enter the COMPANY name. This should match the company name specified during EdgeSight Server setup.

If you are installing the agent on an endpoint device, enter the DEPARTMENT name. If no department name is provided, the agent data will be displayed under the root department.

If you are installing the agent on XenApp, select the operational mode from the **Mode** drop-down menu. If you choose **Basic** mode, some capabilities are not available and no EdgeSight license is consumed. Basic mode is used when installing an EdgeSight for XenApp agent on an Enterprise Edition system.

Click **Next** to display the Agent Location screen.

7. Enter the installation path for the agent or accept the default value. You can browse to select a non-default location.
8. Enter the installation path for the data files or accept the default. You can browse to select a non-default location. Click **Next** to display the Network Settings screen.
9. Enter the server name and port number. These are required fields.
10. The **Automatically configure Windows Firewall for Port 9035** checkbox is selected by default. Enabling this feature automatically configures the firewall for the listen port (the port on which the agent listens for remote connections from the browser displaying the EdgeSight Server console). The firewall must be running, but can either be enabled or disabled. The exclusion is set up for Domain networks. If an exception for Private networks is required, the Domain exception can be used as a template. If you do not want Windows Firewall automatically configured, deselect the checkbox.
11. If an SSL network connection is required, select the **Use SSL** checkbox. (This is equivalent to setting the CONNECTION_FLAGS property.)

12. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server. (This is equivalent to setting the PROXY_ADDRESS, PROXY_PORT, and PASSWORD properties.) Click **Next** to display the Advanced Settings screen.
13. The Advanced Settings screen is only used if you are installing the EdgeSight for Endpoints agent or the EdgeSight for Virtual Desktops agent on virtual desktops in a pool. See [Installing EdgeSight for Monitoring Virtual Desktops](#) for instructions on installing and deploying agents in this type of environment. Click **Next** to display the Ready to Install screen.
14. Click **Install** to begin the installation. (If you need to review or change any settings before installing, use the **Back** button to return to the configuration screens.) When the installation is complete, the Setup Complete screen is displayed.
15. Click **Finish** to complete the installation. The Installer Information dialog is displayed, prompting you to reboot your system so that configuration changes will be applied.
16. Click **Yes** to reboot your machine.

Installing EdgeSight Agents Using the Command Line

The MSI file uses public properties to specify custom install settings. You can edit public properties using the following methods:

- Run the installer user interface (if the property is exposed). This method offers fewer installation options than using the command-line interface. Also, a log file is not created when the user interface is used for installation.
- Create a transform file using a tool such as Orca.
- Specify key/value pairs on the command line. This method allows you to control the full range of installation options, including specifying a log file, as well as being able to specify public properties. The syntax for key/value pairs is *KEY=value*.

See your MSI documentation for syntax rules for property values. The following table lists the public properties used when installing the EdgeSight agent:

Property Name	Description
COMPANY	The company under which data will be displayed on EdgeSight Server. If this property is not specified, the server considers the device unmanaged, and the agent cannot upload data to the server.
DEPARTMENT	The department under which data will be displayed on EdgeSight Server. Special characters are not allowed in the name of an EdgeSight department. If this property is not specified, the device is assigned to the default root department. Note: This property is only available for EdgeSight for Endpoints agents; EdgeSight for Virtual Desktops agents and EdgeSight for XenApp agents use the Farm structure as the department structure.
INSTALLROOT	Location of the main Citrix EdgeSight directory. For example: INSTALLROOT="%programfiles%\citrix\system monitoring\Agent"

DATA_DIR	<p>Location of the Citrix EdgeSight data directory, within quotation marks. If this property is not specified, data files are placed in the default location:</p> <p>%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data\</p> <p>On Microsoft Vista systems, the default path is:</p> <p>%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\</p> <p>Note that the data directory cannot be on a mapped drive.</p>
DELETE_DATA_ON_UNINSTALL	<p>Controls whether agent data files (database and log files) are deleted when the agent is uninstalled.</p> <p>0 = Do not delete files on uninstall</p> <p>1 = Delete files on uninstall</p> <p>Default value is 1.</p>
REMOTE_SECURITY	<p>Determines whether security is enabled for remote connections from the server.</p> <p>0 = Security disabled</p> <p>1 = Security enabled</p> <p>Default value is 1.</p> <p>See the REMOTE_SECURITY_GROUP property for more information on remote device security.</p> <p>Note: This option is deprecated and will be removed in a future version.</p>

<p>REMOTE_SECURITY_GROUP</p>	<p>Local machine group to which the current working user must belong for remote connections from the server. Note that it is the current working user of the machine that is checked, not the user account used to log into the Citrix EdgeSight Server Console.</p> <p>The REMOTE_SECURITY and REMOTE_SECURITY_GROUP properties work together to determine the level of security for remote device access as follows:</p> <p>RemoteSecurity=1, RemoteSecurityGroup=<not set></p> <p>This is the most secure and restrictive setting. In order to display real-time reports based on the agent database, the EdgeSight Server Console user must be a local administrator on the actual device.</p> <p>RemoteSecurity=1, RemoteSecurityGroup=<Active Directory group></p> <p>An Active Directory group must exist or be set up in order to use the REMOTE_SECURITY_GROUP property. Add all EdgeSight users to this group who need access to the real-time reports. This approach allows you to carefully control those users with access to real-time reports.</p> <p>RemoteSecurity=0, RemoteSecurityGroup=<any value></p> <p>This is the least secure setting. This gives all EdgeSight Server Console users the ability to display real-time reports. This setting is generally not recommended.</p>
<p>SYNCH_AD_TREE</p>	<p>Determines whether to synchronize the Active Directory tree with the Citrix EdgeSight department tree.</p> <p>0 = Synchronization disabled</p> <p>1 = Synchronization enabled</p> <p>Default value is 0.</p>

<p>ALLOWSERVEROS</p>	<p>Determine whether to allow an EdgeSight for Endpoints agent to be installed on a system running a server OS.</p> <p>0=No installation on server OS</p> <p>1=Install on server OS</p> <p>Default value is 0.</p> <p>Note: During a silent installation of an EdgeSight for Endpoints agent on a system running a server OS, the install fails unless the ALLOWSERVEROS property is set to 1.</p>
<p>ALLOWVIRTUAL</p>	<p>Determine whether to allow an EdgeSight for Endpoints agent to be installed silently on instances of XenDesktop 4.0 or later.</p> <p>0=No installation on XenDesktop 4.0 or later instance</p> <p>1=Install on XenDesktop 4.0 or later instance</p> <p>Default value is 0.</p> <p>Note: The EdgeSight for Endpoints agent does not collect session-related data on XenDesktop systems. If you wish to collect data relating to XenDesktop, please install the EdgeSight for Virtual Desktop Agent.</p>
<p>NO_CONTROL_PANEL</p>	<p>Determines whether the control panel applet is installed.</p> <p>0=Install control panel applet.</p> <p>1=Do not install control panel applet.</p> <p>Default value is 0.</p> <p>For more information, see Configuring Agents Using the Control Panel.</p>
<p>FUNCTIONALITY_MODE</p>	<p>The operational mode (Basic or Advanced) for an EdgeSight for XenApp agent, as described in “Agent Mode” in Installing EdgeSight Agents. The option values as are follows:</p> <p>1 = Advanced Mode</p> <p>2 = Basic Mode</p>

SHOW_SERVICES_TAB	<p>Determines whether the Service Control tab is displayed on the control panel applet. The tab allows users to enable or disable the Citrix System Monitoring Services.</p> <p>0 = Services tab not displayed.</p> <p>1 = Services tab displayed.</p> <p>Default values are disabled (0) for EdgeSight for Endpoints Agents and enabled (1) for EdgeSight for XenApp Agents.</p> <p>See Configuring Agents Using the Control Panel for more information on the control panel applet.</p>
OVERRIDE_COMPCHECK	<p>Overrides the version check described in “Antivirus Configuration Checking” in Installing EdgeSight Agents. To override the check, specify this property with a value of 1.</p> <p>Note: This property should only be used if you disable the McAfee buffer overflow protection feature as described under "Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent" in the Known Issues topic for your release.</p>
Network Settings	
CONNECTION_FLAGS	<p>0 = No SSL</p> <p>1 = Use SSL</p> <p>Default value is 0.</p>
HTTP_TIMEOUT	<p>Determines how long to wait, in seconds, for a connection or other operation to complete. The default value is 30 seconds.</p>
PROXY_FLAGS	<p>0 - No proxy settings are selected</p> <p>1 - Use proxy</p> <p>3 - Use proxy and non-SSL tunnel (CONNECTION_FLAGS must be set to 0)</p> <p>5 - Use proxy and require authentication (value must be supplied for PROXY_USER)</p> <p>7 - Use proxy and require authentication (value must be supplied for PROXY_USER) and non-SSL tunnel (CONNECTION_FLAGS must be set to 0)</p> <p>Default value is 0.</p>
PROXY_PORT	<p>Port through which the agent communicates with the proxy server. The default port number is 8080.</p>

PROXY_ADDRESS	The hostname or IP address for the proxy server.
PROXY_USER	The user name for the account used to access the proxy server.
PROXY_PASSWORD	Password for access to the proxy server. The password is encrypted before being stored in the registry.
SERVER_NAME	Server to which the agent will report data. This property is required. If no server name is supplied, the agent is unable to upload data to the server.
SERVER_PORT	Port through which the agent communicates with the EdgeSight Server. The default port number is 80.
FIREWALL_EXCEPTION_ALLOWED	Supply a value of 1 to allow Windows Firewall to be automatically configured to exclude the listen port (9035). The firewall must be running, but can either be enabled or disabled. If you do not want the firewall automatically configured, set the value to 0. The default value is 1.
Virtual Desktop Environment Properties	These properties are only used when installing the EdgeSight for Endpoints Agent on virtual desktops in a pool. See Installing EdgeSight for Monitoring Virtual Desktops for more information.
POOLED_INSTALL	Supply a value of 1 to indicate that the agent is to be installed on virtual desktops in a pool. This property must be set to 1 to enable the remaining virtual desktop environment properties.
REMOTE_PATH	The UNC path for the agent data file share.
IMAGE_POOL	The name of the pool in which the virtual desktops will be running. This pool name is case sensitive and must match the pool name specified during the agent database server installation.
DBBROKER_FQDN	The fully-qualified domain name or IP address of the EdgeSight Server which will be acting as the database broker.
BROKER_PORT	The port associated with the EdgeSight Server which will be acting as the database broker.
BROKER_CONNECTION_FLAGS	0 = No SSL 1 = Use SSL
BROKER_PROXY_FLAGS	0 = No proxy 1 = Proxy is of CERN type 2 = Proxy is a non-SSL tunnel to an SSL server
BROKER_PROXY_ADDRESS	The hostname or IP address of the proxy server.
BROKER_PROXY_PORT	Port through which the agent communicates with the proxy server.
BROKER_PROXY_USER	The username used when accessing the proxy server.

BROKER_PROXY_PASSWORD	Password for access to the proxy server. The password is encrypted before being stored in the registry.
-----------------------	---

Use the `msiexec` command to install the agent using the command-line interface. Public properties are specified as *KEY=value* pairs as described earlier in this topic. If a property has a default value, that value is used if the property is not specified on the command line.

When installing an EdgeSight for Endpoints agent using the command line, the following properties should always be specified:

- **SERVER_NAME** - If the server name is not specified, the agent is unable to obtain configuration information or upload data.
- **COMPANY** - If the company name is not specified, the device is considered an unmanaged device and cannot upload data to the server.
- (On a system running a server OS:) **ALLOWSERVEROS** - If this property is not specified, a warning is issued. During a silent installation to a system running a server OS, the install fails unless the **ALLOWSERVEROS** property is set to 1.
- (On a virtual desktop instance running XenDesktop 4.0 or later:) **ALLOWVIRTUAL** - If this property is not specified, a warning is issued. During a silent installation to a virtual desktop instance running XenDesktop 4.0 or later, the install fails unless the **ALLOWVIRTUAL** property is set to 1.

The following is a sample command line for the installation of an EdgeSight for Endpoints agent on a 64-bit desktop system:

```
Msiexec /i EdgeSightEPAgentx64.msi /l logfile.log /q  
SERVER_NAME=Myserver COMPANY=Mycompany DEPARTMENT=Mydept
```

The following is a sample command line for the installation of an EdgeSight for XenApp Agent on a 32-bit system running a server OS:

```
Msiexec /i EdgeSightXAAgent.msi /l logfile.log /q  
SERVER_NAME=Myserver COMPANY=Mycompany DEPARTMENT=Mydept  
ALLOWSERVEROS=1 DATA_DIR="d:\Mydata"
```

The `/i` flag is used to specify the package being installed. The `/l` flag is used to specify the installation log file name. (Capturing an installation log is strongly recommended.) Use the `/q` (quiet) flag to install an agent with no user interaction. For a complete list of standard MSI command-line arguments, open a Command Prompt window and type `msiexec /h` to invoke help, or refer to The Command-Line Options for the Microsoft Windows Installer Tool `Msiexec.exe` at <http://support.microsoft.com/kb/314881>.

Installing the EdgeSight for XenApp Agent in a Streamed Environment

Using the EdgeSight for XenApp Agent, you can implement monitoring of XenApp servers running in a streamed environment using Citrix Provisioning Server for Datacenters 4.5 or later.

The Provisioning Server solution's streaming infrastructure is based on software streaming technology. It allows administrators to create a virtual disk (vDisk) that represents a computer hard drive, and then relocate that vDisk on an OS-Provisioning Server, or on a storage device that has access to a Provisioning Server. Once the vDisk is available, the target device no longer needs its local hard drive to operate; it boots directly across the network. The Provisioning Server streams the contents of the vDisk to the target device on demand, in real time, and the target device behaves as if it is running from its local drive.

Important: Although the operating system and applications are streamed to the target device, the EdgeSight Agent requires a persistent local drive to store its database.

Please review the following installation and configuration guidelines before deploying the EdgeSight for XenApp Agent in this environment.

Prerequisites

EdgeSight Server, Provisioning Server 4.5 or later for Datacenters, and the Citrix License Server for Windows must be installed on their respective machines. For installation instructions, refer to the following product documents:

- [Installing EdgeSight Server](#)
- [Provisioning Server](#) installation documentation
- "Getting Started with Citrix Licensing" under [Licensing Your Product](#)

Installing the EdgeSight Agent on a Master Target Device

After installing the Provisioning Server Target Device software on the master target device, but prior to imaging the system, install the EdgeSight agent. You can install the agent using the command-line or the user interface. In either case, keep in mind the following:

- All target devices associated with a virtual disk (vDisk) must report to the same EdgeSight Server. If a subset of machines is to report to a different EdgeSight Server, create a new vDisk for these devices.

- EdgeSight Agents detect when the vDisk is in private mode and will not start. This capability eliminates the need to set the EdgeSight agent service start mode to manual.
- If the master target device has only one disk drive, the installer will not allow a nonexistent drive to be specified. Registry and file system changes are required before master target imaging. See “Installation on a Master Target Device with a Single Disk” later in this topic for more information.

Installing the Agent Using the Command-Line Interface

The SERVER_NAME and COMPANY parameters should always be specified to ensure that configuration information can be obtained from the server and that data can be uploaded to the server. The following sample command line also shows the use of the DATA_DIR parameter to select the data files folder. Note that the data directory cannot be on a mapped drive.

```
miexec.exe /i EdgeSightXAAgent.msi /l logfile.log /q  
SERVER_NAME=rsbetx COMPANY=Mycompany DATA_DIR="d:\Citrix\System  
Monitoring\Mydata"
```

Installing the Agent Using the User Interface

In the Agent Location dialog, be sure to install the EdgeSight agent on the virtual disk (vDisk). The default location can be used. Change the data folder to a location on the physical disk that will be in each target device. Note that the data directory cannot be on a mapped drive.

In the Network Settings dialog, specify the server name and port number for the EdgeSight Server. All target devices that use the vDisk will report to this server. If a subset of target devices is going to report to a different EdgeSight server, a separate vDisk must be created for those devices. (Do not change the network settings on an individual device; these changes are not persisted if the device is rebooted.)

Installation on a Master Target Device with a Single Disk

If the master target device has only one disk drive, the installer will not allow you to specify a data folder on a nonexistent drive. In this case, perform the installation using the default values and then edit the registry and file system when the installation completes:

1. Within the registry, navigate to the key `HKLM\Software\Citrix\System Monitoring\Agent\Core\4.00` and change the `DataPath` to the appropriate location on the physical disk of the target devices.

2. Within the file system, navigate to %ProgramFiles%\Citrix\System Monitoring\Agent\Core\Firebird and locate aliases.conf.
3. Open aliases.conf in a text editor and change the `RSData` entry to match the location of the data folder on the physical disk of the target devices. For example: `RSData = D:\Citrix\System Monitoring\Data\RSData.fdb`

Imaging the Master Target Device Disk

Image the disk of the master target device.

Configuring Target Devices

Each target device must have a physical disk drive. The drive must have an NTFS partition that is visible to the streamed OS.

Set the boot order of the target device to boot from the network first.

Boot the target device from the shared vDisk. After booting the target device, the Citrix System Monitoring Agent service should be running and the service's data should be present on the target device's disk drive. If you need to troubleshoot a specific target device, registry changes for additional tracing should be made on the device, not on the vDisk. Note that these changes are not persisted if the device is rebooted.

Configuring Agents Using the Control Panel

If you need to reconfigure connection settings for agent to server communication after installation, use the Citrix System Monitoring Agent control panel applet. You must have Administrator privileges on the machine to launch the applet. To use the applet:

1. From the **Start** menu, choose **Settings > Control Panel** and select **Citrix System Monitoring Agent** to display the Citrix System Monitoring Agent Settings dialog.
2. Edit the Citrix EdgeSight Server address and port number as required.
3. Select the **Use SSL encryption** checkbox if the Citrix EdgeSight Server is SSL enabled. To be SSL enabled, a valid SSL certificate issued by a trusted certificate authority must be present on the server running the Citrix EdgeSight Web site. If SSL support is enabled, all agent to server communications must be over SSL. If an agent attempts to connect to an SSL-enabled server without using SSL, an error is generated and the data upload is rejected.
4. Select the **Use a proxy server** checkbox if a proxy server is used. Enter the proxy server address and port and indicate whether the server is a non-SSL tunnel and whether authentication is required. Supply the authentication username and password if required.
5. If an EdgeSight for XenApp agent is installed on a machine running XenApp Enterprise, you can select the **Mode** tab and change the agent mode (Basic or Advanced). Note that this tab is not displayed on XenApp Platinum systems. For more information on agent modes, see “Agent Mode” in [Installing EdgeSight Agents](#).
6. When you have made all required settings changes, click **OK** to apply the changes and close the dialog. If the Service Control tab has been enabled on the control panel applet, you can disable or enable the Citrix System Monitoring Service and the Firebird Server - CSMinstance service. Disabling these services stops the services and sets the startup type to disabled. Enabling the services starts the services and sets the startup type to automatic.

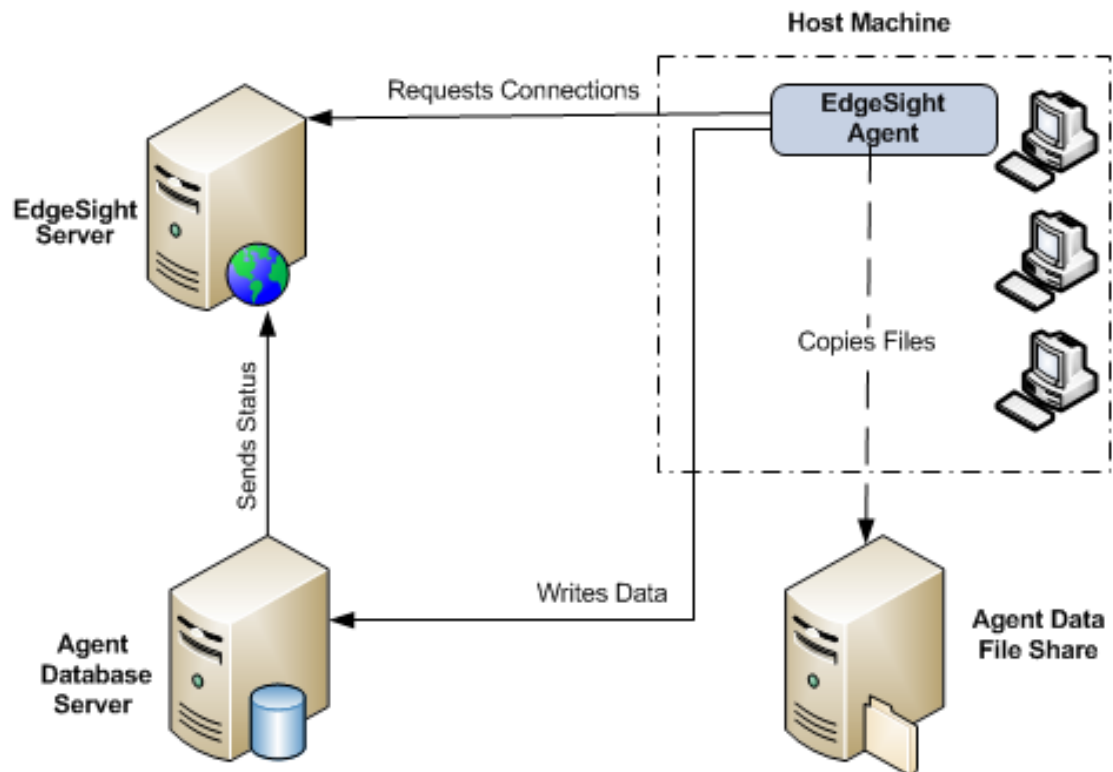
Important: The Service Control capability is intended for use in the event that you suspect that an EdgeSight Agent is causing performance or software compatibility problems. By using the Service Control feature, you can disable services and keep them from restarting. If you uninstall the agent when a problem occurs, you may lose data which may help in resolving the problem.

The Service Control tab is enabled by default for EdgeSight for XenApp agents, but it is disabled by default for EdgeSight for Endpoints agents.

The Service Control tab can be displayed by setting the `SHOW_SERVICES_TAB` parameter to 1 during agent installation, or by setting the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\System Monitoring\Agent\Core\4.00\Control Panel\AllowServiceControl` registry key to 1.

Installing EdgeSight for Monitoring Virtual Desktops

When monitoring physical endpoint machines, EdgeSight Agents store performance and availability data in a local database. Because virtual desktops in a pool are not preserved across reboots, agents must store data externally on a database server and a file share. The following figure shows the components required for virtual desktop monitoring.



- **EdgeSight Server** - In addition to displaying reports and providing an interface for administration and configuration, EdgeSight Server includes database broker components which respond to agent requests for a connection string to an EdgeSight Agent Database Server.
- **EdgeSight Agent Database Server** -The EdgeSight Agent Database Server provides storage for data collected by EdgeSight Agents running on virtual desktops in a pool. During installation you will be asked to specify the name of the pool and the name of the EdgeSight Server which will act as the database broker. (Multiple agent database servers can be associated with a pool.) Once the agent database server has been installed, it registers with the EdgeSight Server and regularly reports its operational status.

- **Agent Data File Share** - The agent data file share provides storage for files such as log files and INI files which are not stored on the EdgeSight Agent Database Server. It is recommended that you set up your file share on either the EdgeSight Server or on an Agent Database Server machine.

Note: In the above diagram, Agent Data File Share is shown separately to indicate that it is not part of the EdgeSight Server or EdgeSight Agent Database Server installation and requires separate setup.

- **EdgeSight for Virtual Desktops Agent** - Initially, the EdgeSight Agent requests a connection string to an EdgeSight Agent Database Server. Once the agent is operational, it writes data to the agent database server and copies files to the agent data file share.
1. Install the EdgeSight Server that will also act as the broker for remote agent databases. See [Configuring Database Brokers](#) for details.
 2. Install one or more agent database servers for each pool. See [Installing the Agent Database Server](#) for details.
 3. Setup a file share for agent data that does not reside in the database. See [Setting Up the Agent Data File Share](#) for details.
 4. Install the EdgeSight Agent on the disk to be used by virtual desktops. See [Installing the Agent](#) for details. For overall system requirements for a virtual desktop environment, see “Virtual Desktop Monitoring Requirements” in [System Requirements](#).

Configuring Database Brokers

EdgeSight Server software includes components that assist agents running on virtual desktops to locate and connect to remote databases. When you install the EdgeSight Server Website, it additionally installs Web services that perform the following operations:

- Broker database connections for agents running on virtual desktops in a pool
- Monitor the status of available agent databases

These components are installed by default; you do not have to explicitly select or configure them. This allows you to easily designate a different EdgeSight Server as the database broker.

If you have multiple EdgeSight Server installations, you need only select one to act as the database broker, though you may designate others if you wish. The EdgeSight Server that will act as the database broker is selected when you install the agent database server, as described in [Installing the Agent Database Server](#). Note that if an EdgeSight Server is not brokering database connections, no status information will be displayed on the Agent Database Broker pages of the server console. See [Installing EdgeSight Server](#) for detailed instructions on installing EdgeSight Server software.

Installing the Agent Database Server

The agent database server can be installed on a Windows physical or virtual server-class machine. The installation creates a database monitor. An agent database is created when an agent is brokered to the agent database server. The database stores data written by an EdgeSight Agent, while the database monitor reports database availability and status to the EdgeSight Server acting as a database broker. If a firewall is installed on the machine, port 9037 must be open to allow communication with EdgeSight agents. Each agent database server can support one image pool.

During installation you will be asked to specify the name of the pool and the name of the EdgeSight Server which will act as the database broker. Typical disk space usage is generally 70 MB per virtual desktop for the databases on a single disk. After the installation is complete, the database monitor reports the availability of the agent database server to the database broker.

1. Insert the media.
2. Select **EdgeSight Component Installers**.
3. Select **EdgeSight Agent Database Server** to display the installer Welcome page.
4. Click **Next** to display the End User License Agreement page.
5. After reading the license agreement, select the **I accept** radio button and click **Next** to display the Network Settings page.
6. Enter the broker name and port. The broker name is the name of the machine hosting the previously installed EdgeSight Server, which includes the database broker components. You can also enter an IP address or fully qualified domain name.
7. The **Automatically configure Windows Firewall for Port 9037** checkbox is selected by default. Enabling this feature automatically configures the firewall for the database listen port (the port on which the agent database server listens for remote connections from the database broker). The firewall must be running, but can either be enabled or disabled. The exclusion is set up for Domain networks. If an exception for Private networks is required, the Domain exception can be used as a template. If you do not want Windows Firewall automatically configured, deselect the checkbox.
8. If an SSL network connection is required, select the **Use SSL** checkbox.
9. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server.
10. After specifying the network settings, click **Next** to display the Agent Location screen.
11. Enter the installation path for the agent database server or accept the default value. You can browse to select a non-default location.
12. Enter the installation path for the data files or accept the default. You can browse to select a non-default location.

13. Enter a name for the pool hosting the agents which will store data on the agent database server. You can choose any pool name. For ease of use, you may want to choose one that corresponds to the XenDesktop desktop group name.
14. Click **Next** to display the Ready to Install screen.
15. Click **Next** to begin the installation and display the Performing Installation screen. When the installation is complete, the Setup Complete page is displayed.
16. Click **Finish** to exit the setup wizard.

Setting Up the Agent Data File Share

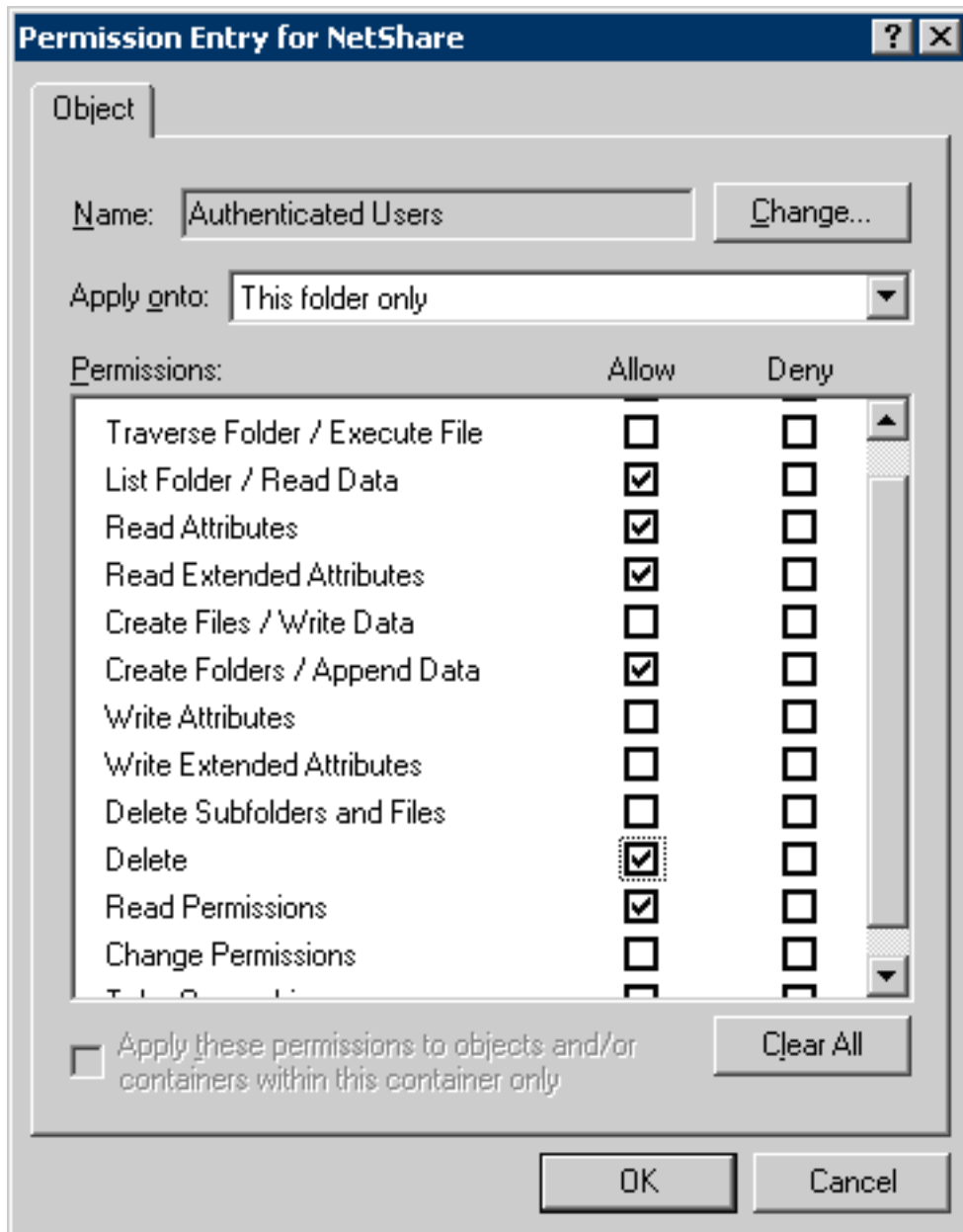
Some agent data are not stored in the agent database, such as log files and INI files. Therefore, agents running on virtual desktops require access to an external file share. The file share must be configured with permissions allowing authenticated users to create subdirectories that will contain the files, plus settings. The disk space needed is minimal and the file copies are small and infrequent. It is recommended that you set up your file share on either the EdgeSight Server or on an agent database server machine.

On Windows 2003 Systems

The permissions required include both the file share permissions and the NTFS file system permissions. To create an agent data file share and set all permissions on a Windows 2003 system:

1. Create a new folder. The file share should not be located on a specific user's desktop. Record the folder UNC path for use during the agent installation process.
2. Right click on the folder name and select **Properties** from the popup menu to display the Properties dialog.
3. Select the **Sharing** tab. Select the **Share this folder** radio button.
4. Click the **Permissions** button to display the Permissions dialog.
5. Click **Add** to display the Select Computer, User, or Group dialog.
6. Enter **Authenticated Users** in the **Enter object name to select** field. Click **OK**.
7. Select the **Authenticated Users** group.
8. Ensure that the **Change** and **Read** permissions are selected and click **OK**.
9. Select the **Security** tab and click the **Advanced** button to display the Advanced Security Settings dialog.
10. Deselect the checkbox which enables child objects to inherit permission entries from the parent. (The specific checkbox label may vary based on the operating system.) When this setting is disabled, a Security dialog is displayed advising you that permission entries will no longer be inherited. Click **Remove**.
11. Click **Add** to display the Select Computer, User, or Group dialog.
12. Enter **Authenticated Users** in the **Enter object name to select** field. Click **OK** to display the Permission Entry dialog.
13. Select **This folder only** from the **Apply onto** drop down menu.
14. Ensure that the following permissions are allowed:

- List Folder / Read Data
- Read Attributes
- Read Extended Attributes
- Create Folders / Append Data
- Delete
- Read Permissions



15. Click **OK** on all open dialog boxes.

On Windows 2008 Systems

To create an agent data file share and set all permissions on a Windows 2008 system:

1. Create a new folder. The file share should not be located on a specific user's desktop. Record the folder UNC path for use during the agent installation process.
2. Right click on the folder name and select **Properties** from the popup menu to display the Properties dialog.
3. Select the **Sharing** tab. Select the **Share** button to display the File Sharing dialog.
4. Enter **Authenticated Users** in the text entry field. Click **Add**.
5. Select the **Authenticated Users** group and click on **Contributor** in the drop-down menu.
6. Click **Share**. When the operation is complete, click **Done**.
7. Select the **Security** tab, select **Authenticated Users** from the list of groups and user names. Click the **Advanced** button to display the Advanced Security Settings dialog.
8. Select **Authenticated Users** from the list of permission entries and click **Edit** to display the Advanced Security Settings dialog.
9. Deselect the checkbox which enables child objects to inherit permission entries from the parent. (The specific checkbox label may vary based on the operating system.) When this setting is disabled, a Security dialog is displayed advising you that permission entries will no longer be inherited. Click **Remove**.
10. Select **Authenticated Users** from the list of permission entries and click **Edit** to display the Permission Entry dialog.
11. Select **This folder only** from the **Apply to** drop down menu.
12. Ensure that the following permissions are allowed:
 - List Folder / Read Data
 - Read Attributes
 - Read Extended Attributes
 - Create Folders / Append Data
 - Delete
 - Read Permissions
13. Click **OK** on all open dialog boxes.

Prerequisites for Installing EdgeSight Agents

Before installing the agent in a virtual desktop environment, you must perform the following tasks:

1. Ensure that you have the information required during agent installation.
2. Place the group of virtual desktops in maintenance mode and then shut them down.
3. Set the vDisk access mode to private.

Note: This procedure assumes that you are working with an existing master image. You can also install the agent as part of creating a master image prior to sharing the image out to the pool.

Shutting Down Virtual Desktops

Important: Before shutting down virtual desktops, ensure that they are not in use to avoid loss of data.

Before installing the agent in a virtual desktop environment, you must ensure that the virtual desktops are in maintenance mode and are then shut down. To set the virtual desktops to maintenance mode and shut them down:

1. Log on to the Desktop Delivery Controller (DDC) for the target desktop group and open the Citrix Access Management Console.
2. Navigate to **Citrix Resources > Desktop Delivery Controller > FarmName > Desktop Groups** and click on the target group to display a list of the virtual desktops.
3. Select all desktops in the group and right click on the group to display the pop-up menu. Select **Enable maintenance mode** to temporarily stop connections to the desktops.
4. Right click on the group again and select **Shutdown/suspend** from the pop-up menu to display the Shutdown/suspend dialog.
5. Select **Shut down** from the drop-down menu and click **OK**. (You may need to refresh the display to update the status displayed for the desktops.)

Setting the vDisk Access Mode to Private

You must set the access mode property for the vDisk associated with the target desktop group.

1. Log on to the Provisioning Server associated with the vDisk on which the EdgeSight Agent will be installed and start the Provisioning Server Console.
2. Navigate to **FarmName** > **Stores** and select the store associated with the target vDisk.
3. Right click on the vDisk and select **Properties** from the pop-up menu.
4. Click on the **Edit file properties** button to display the vdisk File Properties dialog.
5. Select the **Mode** tab.
6. Select **Private access (single device, R/W access)** from the **Access Mode** drop down menu and click **OK**.
7. Click **OK** in the vdisk File Properties dialog.

Information Required During Agent Installation

Ensure that you have the following information at hand before installing the agent software on the master image:

- The UNC path name of the agent data file share. The Network Service that will be running on desktops will need to be able to create directories and copy files to this share.
- The fully-qualified domain name or IP address of the EdgeSight Server that will be acting as the database broker. In addition to the server name you can specify the port and SSL or proxy server information, if used.
- The name of the pool in which the virtual desktops will be running. This pool name is case sensitive and must match the pool name specified during the agent database server installation. The pool name corresponds to the XenDesktop desktop group name.

Installing the Agent

You install the EdgeSight for Virtual Desktops Agent or the EdgeSight for Endpoints Agent on the master image. During the installation, you indicate that the agent is being installed on virtual desktops. After the agent installation is complete, you must reboot your master image.

Software Configuration Tasks

You may need to change the configuration of some software, such as antivirus software or personal firewalls, on machines which will run the EdgeSight Agent and will host the agent database server and the agent data file share to ensure proper operation. You can perform these configuration tasks before or after installing the EdgeSight Agent. For more information, see [Configuring Third Party Software](#).

If you are running a firewall on the machine hosting the agent database server, the port used to communicate with EdgeSight agents must be open. The default port is 9037.

Antivirus Configuration Checking

Due to the manner in which buffer overflow protection was implemented in McAfee VirusScan 8 or 8i with Patch 10, this feature which may conflict with the operation of the EdgeSight Agent. (In later versions of McAfee VirusScan, this feature was implemented differently and does not conflict with EdgeSight Agent operation.) The EdgeSight Agent installer checks for McAfee 8 or 8i with Patch 10 or below on the target machine. If the EntApi.dll file is present with version 8.0.0.277 and below, the installation exits with an error. The check is performed on both full UI and unattended installations. In a command-line installation, the check can be omitted from the installation process by specifying the `OVERRIDE_COMPCHECK` property with a value of 1.

Note: The `OVERRIDE_COMPCHECK` property should only be used if you disable the McAfee buffer overflow protection feature as described under "Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent" in the [Known Issues in EdgeSight 5.4](#) topic.

Agent Installation Methods

The MSI file uses public properties to specify custom install settings. You can set public properties using the following methods:

- Run the installer user interface (if the property is exposed). This method offers fewer installation options than using the command-line interface. Also, a log file is not

created when the user interface is used for installation.

- Create a transform file using a tool such as Orca.
- Specify key/value pairs on the command line. This method allows you to control the full range of installation options, including specifying a log file, as well as being able to specify public properties. The syntax for key/value pairs is *KEY=value*.

See your MSI documentation for syntax rules for property values. See [Installing EdgeSight Agents Using the Command Line](#) for definitions of the public properties used when installing the EdgeSight agent.

Installing an Agent Using the User Interface

Note that not all public properties listed in [Installing EdgeSight Agents Using the Command Line](#) are exposed when installing using the user interface. Properties not explicitly set from the user interface are set to their default value if one exists. To install an agent using the user interface:

1. Insert the media.
2. Select **EdgeSight Agent Installers**.
3. Select **EdgeSight for Virtual Desktops Agent** or **EdgeSight for Endpoints Agent** to display the Welcome screen.
4. Click **Next** to display the License Agreement screen.
5. After reading the license, select the **I accept** radio button and click **Next** to display the Company Information screen.
6. Enter the company name. If you are installing an EdgeSight for Virtual Desktops agent for monitoring instances of XenDesktop 4.0 or later, the department field cannot be set because the department is determined by the XenDesktop Farm structure. Click **Next** to display the Agent Location screen.
7. Enter the installation path for the agent or accept the default value. You can browse to select a non-default location.
8. Enter the installation path for the data files or accept the default. You can browse to select a non-default location. Click **Next** to display the Network Settings screen.
9. Enter the server name and port number. These are required fields.
10. If an SSL network connection is required, select the **Use SSL** checkbox. (This is equivalent to setting the CONNECTION_FLAGS property.)
11. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server. (This is equivalent to setting the PROXY_ADDRESS, PROXY_PORT, and PASSWORD properties.) Click **Next** to display the Advanced Settings screen.
12. Select the **Configure the agent for virtual desktops** checkbox.

13. In the **Remote UNC Path** field, enter the UNC path for the agent data file share, for example `\\Myserver.mydomain.com\AgentFiles`. For information on setting up the file share, see [Setting Up the Agent Data File Share](#).
14. In the **Pool Name** field, enter the name of the pool in which the virtual desktops will be running. This pool name is case sensitive and must match the pool name specified during the agent database server installation, as described in [Installing the Agent Database Server](#).
15. In the **Database Broker** field, enter the fully-qualified domain name of the EdgeSight Server which will be acting as the database broker. (The database broker components are installed on every EdgeSight Server and cannot be installed separately or moved.)
16. If an SSL network connection is required, select the **Use SSL** checkbox.
17. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server. Click **Next** to display the Ready to Install screen.
18. If you need to review or change any settings before installing, use the **Back** button to return to the configuration screens.
19. Click **Install** to begin the installation. When the installation is complete, the Setup Complete screen is displayed.
20. Click **Finish** to complete the installation. The Installer Information dialog prompts you to reboot your system so that configuration changes will be applied.
21. Click **Yes** to reboot your machine. It is recommended that you flush the DNS cache after rebooting the machine (`ipconfig /flushdns`). This can help prevent errors related to DNS caching when the agent initially accesses the network.

Installing an Agent Using the Command-Line Interface

Use the `msiexec` command to install the agent using the command-line interface. Public properties are specified as `KEY=value` pairs as described in [Installing EdgeSight Agents Using the Command Line](#). If a property has a default value, that value is used if the property is not specified on the command line. When performing an installation in a virtual desktop environment using the command line, the following properties should always be specified:

- `SERVER_NAME`—If the server name is not specified, the agent is unable to obtain configuration information or upload data.
- `COMPANY`—If the company name is not specified, the device is considered an unmanaged device and cannot upload data to the server.
- `POOLED_INSTALL`—This flag and the following properties are required so that the agent can communicate with the database broker components of EdgeSight Server and can copy and retrieve files from the agent data file share.
- `REMOTE_PATH`

- IMAGE_POOL
- DBBROKER_FQDN
- BROKER_PORT

ALLOWSERVEROS should be specified if you attempt to install a Citrix EdgeSight for Endpoints agent on a system running a server OS. If this property is not specified, a warning is issued. During a silent installation to a system running a server OS, the install fails unless the ALLOWSERVEROS property is set to 1.

ALLOWVIRTUAL should be specified if you attempt to install an EdgeSight for Endpoints agent on a virtual desktop instance running XenDesktop 4.0 or later. If this property is not specified, a warning is issued. During a silent installation to a virtual desktop instance running XenDesktop 4.0 or later, the install fails unless the ALLOWVIRTUAL property is set to 1.

The following is a sample command line for the installation of an EdgeSight for Endpoints agent on a 64-bit virtual desktop system:

```
Msiexec /i EdgeSightEPAgentx64.msi /l logfile.log /q  
SERVER_NAME=Myserver COMPANY=Mycompany DEPARTMENT=Mydept  
POOLED_INSTALL=1 REMOTE_PATH="\\Myserver.mydoain.com\AgentFiles"  
IMAGE_POOL=Pool2 DBBROKER_FQDN=Myserver.dom1.com BROKER_PORT=80
```

The `/i` flag is used to specify the package being installed. The `/l` flag is used to specify the installation log file name. (Capturing an installation log is strongly recommended.) Use the `/q` (quiet) flag to install an agent with no user interaction. For a complete list of standard MSI command-line arguments, open a Command Prompt window and type `msiexec /h` to invoke help, or refer to The Command-Line Options for the Microsoft Windows Installer Tool Msiexec.exe at <http://support.microsoft.com/kb/314881>.

Deploying the Agent to Virtual Desktops in a Pool

To deploy the agent to the virtual desktops in a pool, perform the following tasks:

1. Shut down the master image.
2. Set the access mode property for the vDisk associated with the target desktop group to **Standard Image**.
3. Disable maintenance mode on the desktop group.

Note: This procedure assumes that you are working with an existing master image. You can also install the agent as part of creating a master image prior to sharing the image out to the pool. If you are not working with an existing vDisk, create the vDisk at this point in the procedure.

Shutting Down the Master image

The master image must be shut down so that the access mode property for the vDisk can be changed.

Setting the vDisk Access Mode

You must set the access mode property for the vDisk associated with the target desktop group.

1. Log on to the Provisioning Server associated with the master image on which the EdgeSight Agent was installed and start the Provisioning Server Console.
2. Navigate to **FarmName** > **Stores** and select the store associated with the target vDisk.
3. Right click on the vDisk and select **Properties** from the pop-up menu.
4. Click on the **Edit file properties** button to display the vdisk File Properties dialog.
5. Select the **Mode** tab.
6. Select **Standard Image (multi-device, write-cache enabled)** from the **Access Mode** drop down menu and click **OK**.
7. Click **OK** in the vdisk File Properties dialog.

Disabling Maintenance Mode

To enable normal operation by the virtual desktops, you must ensure that maintenance mode is disabled. To disable maintenance mode for the desktop group:

1. Log on to Desktop Delivery Controller (DDC) for the target desktop group and open the Citrix Access Management Console.
2. Navigate to **Citrix Resources > Desktop Delivery Controller > FarmName > Desktop Groups** and click on the target group. A list of the virtual desktops is displayed.
3. Select all desktops in the group and right click on the group to display the pop-up menu. Select **Disable maintenance mode**.

Post-Installation Configuration

You may need to change incorrect configuration settings using the agent's control panel application.

Agent Database Connection Acquisition

When you configure the agent for virtual desktops, file monitor components are installed which manage copying files to and retrieving files from the agent data file share. The agent is configured to contact the database broker to receive a database connection string. If it fails to get a database connection, it shuts down and writes error information to the local SYS_EVENT_TXT.TXT log. If the file monitor components are functioning properly, a copy of the log file will also be placed on the agent data file share. You can change incorrect configuration settings using the agent's control panel application. However, you must make those changes on the master image in order for them to be propagated to all desktops.

Configuring Agents Using the Control Panel

If you need to reconfigure connection settings for agent to server communication after installation, use the Citrix System Monitoring Agent control panel applet. You must have Administrator privileges on the machine to launch the applet.

In a virtual desktop environment, any changes to these settings must be made on the master image and then deployed to the pool.

The Service Control tab is disabled by default for EdgeSight for Virtual Desktops and EdgeSight for Endpoints agents. The Service Control tab can be displayed by setting the SHOW_SERVICES_TAB parameter to 1 during agent installation, or by setting the HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\System Monitoring\Agent\Core\4.00\Control Panel\AllowServiceControl registry key to 1.

To use the applet:

1. From the **Start** menu, choose **Settings > Control Panel** and select **Citrix System Monitoring Agent** to display the Citrix System Monitoring Agent Settings dialog.
2. Select the **Remote Share** tab. Edit the UNC path to the agent data file share as required.
3. Select the **EdgeSight Server** tab. Edit the Citrix EdgeSight Server address and port number as required.
4. Select the **Use SSL encryption** checkbox if the Citrix EdgeSight Server is SSL enabled. To be SSL enabled, a valid SSL certificate issued by a trusted certificate authority must be present on the server running the Citrix EdgeSight Web site. If SSL support is enabled, all agent to server communications must be over SSL. If an agent attempts to connect to an SSL-enabled server without using SSL, an error is generated and the data

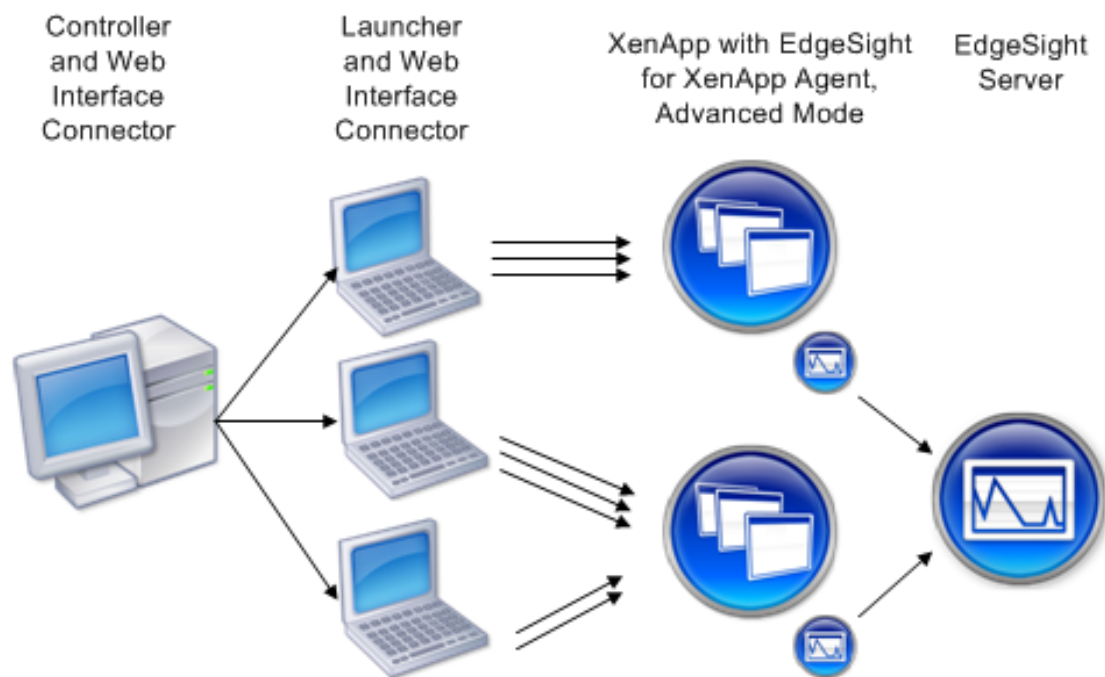
upload is rejected.

5. Select the **Use a proxy server** checkbox if a proxy server is used. Enter the proxy server address and port and indicate whether the server is a non-SSL tunnel and whether authentication is required. Supply the authentication username and password if required.
6. Select the **Broker Server** tab. Edit the address and port number for the EdgeSight Server acting as the database broker as required. You can also edit SSL and proxy server settings as described in steps 4 and 5.
7. When you have made all required settings changes, click **OK** to apply the changes and close the dialog.

Important: The Service Control capability is intended for use in the event that you suspect that an EdgeSight Agent is causing performance or software compatibility problems. By using the Service Control feature, you can disable services and keep them from restarting. If you uninstall the agent when a problem occurs, you may lose data which may help in resolving the problem.

Installing EdgeSight Active Application Monitoring Software

EdgeSight AAM depends on the deployment of several software components. For AAM component system requirements, see “Active Application Monitoring Requirements” in [System Requirements](#).



1. Install EdgeSight Server, adhering to the system requirements listed in “Server Requirements” in [System Requirements](#).
2. Install the AAM Controller and Launcher, adhering to the system requirements listed in “Active Application Monitoring Requirements” in [System Requirements](#). These components can be installed on the same machine or on different machines.
3. Optionally, install the Web Interface Connector. This component is required if users will be connecting to XenApp systems using the XML service. The Web Interface Connector requires the installation of Microsoft Visual J# .NET Redistributable Package.
4. Install the EdgeSight for XenApp Agent on each XenApp system to be tested, adhering to the system requirements listed in “Agent Requirements” in [System Requirements](#). The agent must be installed in Advanced Mode to ensure that AAM-related alerts can be generated.

The Launcher is installed as a service (Citrix EdgeSight Launcher Service). The default location for Launcher installation is:

%ProgramFiles%\Citrix\Citrix EdgeSight Simulation\LauncherService.exe

Launchers and the Controller use port 18747 to communicate.

After deploying the software components, you can perform the following tasks, as described in EdgeSight Active Application Monitoring Help and EdgeSight Server Online Help:

- Configure the systems to be tested, as well as the systems hosting the Controller and Launchers.
- Using the Controller, create a script, including monitoring points, and create virtual users.
- Using the EdgeSight Server Console, create Application Response Time and Application Response Failure alerts for real-time notification of application response times that exceed thresholds or application response failures.
- Using the EdgeSight Server Console, monitor applications under test using the Application Response Time and Application Response Failure historical reports.

Installing the Active Application Monitoring Components

Important: If you previously installed the AAM components included with the EdgeSight 5.3 or 5.4 release, you will be prompted to uninstall those components before running the EdgeSight AAM 5.3 Service Pack 2 installer.

Use the following steps to initially install the software:

1. Insert the media or run Autorun.
2. Select **EdgeSight Component Installers**.
3. Select **EdgeSight Active Application Monitoring Installation** to display the Welcome screen.
4. Click **Next** to display the License Agreement screen.
5. After reading the license, select **I accept** and click **Next** to display the Installation Type screen.
6. Select the type of installation you want to perform. If you selected Custom, go to Step 7. If you selected Typical or Complete, skip to Step 8.
 - Typical - Install the Controller and Launcher
 - Custom - Select the components you want to install from Controller, Launcher, and Web Interface Connector. When you use the Web Interface Connector, it must be installed on the Controller and Launcher. The Web Interface Connector allows users to connect to applications made available through the XML Service. This feature requires the Visual J# Version 2.0 Redistributable Package available from Microsoft at <http://msdn2.microsoft.com/en-us/vjsharp/default.aspx>.

- Complete - Install the Controller, Launcher, and Web Interface Connector.
7. By default, all components are enabled. To disable installation of a component, click the component and select **Entire feature will be unavailable**. Click **Disk Usage** to display disk space availability, or click **Reset** to return to the default component selections. When you have completed feature selection, click **Next**.
 8. The system prompts for a password. This password will be required when using each Launcher and the Controller. The password must be at least 8 characters in length and should match the passwords set on all Launcher machines to be used in the test.
 9. Click **Install** to install the software and display the Performing Installation Tasks screen. The Installation Complete screen is displayed after the software is installed.
 10. Click **Finish** to exit the Setup Wizard.
 11. After the installation is complete, go to **Citrix > Citrix EdgeSight Active Application Monitoring > AAM Controller** and log in using the previously specified password. Select **Help > Help Topics** to display online help. The help file includes information about configuring Controllers, Launchers, and XenApp systems under test.

Configuring Third Party Software

In some cases, you may need to perform software configuration tasks to ensure that EdgeSight works properly in your environment. Review the following guidelines and implement the recommendations as required. In addition, review the [Known Issues in EdgeSight 5.4](#).

Configuring Antivirus Software

You must configure antivirus software running on your EdgeSight Server and all managed devices (machines running EdgeSight Agent) to exclude specific processes and files. If these files and processes are not excluded, communications between the agents and the server may be disrupted, and performance on monitored devices can be degraded.

Note: The paths and filenames provided are based on default installation values for EdgeSight and other software components. If you have specified non-default paths and filenames, use the values applicable to your installation. You can use the About page on the EdgeSight Server Console to identify installation paths and filenames on the server.

To configure antivirus software on devices running EdgeSight Agent:

- Ensure that the following agent service, which is a script host, is not subject to script blocking:

`%ProgramFiles%\Citrix\System Monitoring\Agent\Core\rscorsvc.exe`

- Exclude the following folder. This folder contains the EdgeSight database, which is highly transactional, along with log files and temporary files:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\` for Microsoft Vista and Windows Server 2008 systems

`%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data\` for all other systems

If you have agents installed in a virtual desktop environment, exclude the following:

- The data folder on the EdgeSight Agent Database Server:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\` for Windows Server 2008 systems

`%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data\` for all other systems

- Agent data file share. See [Setting Up the Agent Data File Share](#) for more information on the file share configuration.

To configure antivirus software on your EdgeSight Server:

- Ensure that the following files, which are script hosts, are not subject to script blocking:

`%CommonProgramFiles%\Citrix\System Monitoring\Server\RSSH\RSshApp.exe`

`%CommonProgramFiles%\Citrix\System Monitoring\Server\RSSH\RSshSvc.exe`

- Exclude the following folder, which contains the Citrix EdgeSight Web server:

`%ProgramFiles%\Citrix\System Monitoring\Server`

- Exclude the SQL DB folder:

`%ProgramFiles%\Microsoft SQL Server\MSSQL\Data\`

- Exclude the IIS Web Site Log files:

`%SystemRoot%\SYSTEM32\Logfiles`

Configuring Firewalls

The listen port on the client machine (port 9035) must be open. This is the port on which the agent listens for remote connections from the browser displaying the Citrix EdgeSight console. There is an option during agent installation to automatically set a Windows Firewall exception for the listen port if the firewall is running (enabled or disabled).

If a firewall is installed on the machine hosting the EdgeSight Agent Database Server, port 9037 must be open to allow communication with EdgeSight Server. There is an option during agent database server installation to automatically set a Windows Firewall exception for the listen port if the firewall is running (enabled or disabled). The EdgeSight Agent Database Server is only installed when using the EdgeSight for Endpoints agent to monitor virtual desktops.

Certain types of ports must be opened to allow EdgeSight Server (specifically the User Troubleshooter) to communicate with XenApp. EdgeSight Server uses MFCOM to communicate with XenApp servers. MFCOM in turn uses DCOM and requires that RPC ports are opened on the XenApp server.

Upgrading EdgeSight

Upgrading or Uninstalling EdgeSight Server

You can directly upgrade from EdgeSight Server 5.3 to EdgeSight Server 5.4. Upgrades from Technology Preview releases are not supported.

Note:

- EdgeSight Server 5.4 and EdgeSight Server 5.3 require either SQL Server 2008 R2 or SQL Server 2005. If you are upgrading EdgeSight Server from a release prior to EdgeSight 5.2 using SQL Server 2000, you will also need to upgrade your SQL Server installation.
- Support for the EdgeSight Virtual Desktop Agent is not enabled by default when you upgrade EdgeSight Server from a release prior to EdgeSight 5.2. To enable support after upgrading, open the EdgeSight Server Console and go to **Configure > Server Configuration > Settings** and set EdgeSight for XenDesktop Support to **On**.

Important: You should back up your EdgeSight database before performing an EdgeSight Server upgrade. Optionally, you may want to reboot your EdgeSight Server so that all EdgeSight processes are restarted, providing a known state from which to upgrade. Also, the EdgeSight Server should be upgraded before upgrading the associated EdgeSight agents.

Each time you invoke server setup, the MSI file checks for existing versions of the Citrix EdgeSight database and Web server components.

The time it takes to perform an upgrade may be affected by size of the database and the distribution of the database file group. Additional time may be required to perform file group moves during the upgrade.

If you are performing a database-only upgrade on a system hosting both the EdgeSight Web site and database, turn off IIS on the system before performing the upgrade. This will prevent EdgeSight from attempting to process data uploads and alerts at the same time that the database is being updated. In the case of a full update, however, IIS must be running in order to allow an IIS reset as part of the installation process.

1. Open the EdgeSight Server Console.
2. Select the **Configuration** tab.
3. Navigate to **Server Configuration > Settings** and select the **Agent Support** tab.
4. Set **EdgeSight for XenDesktop Support** to **On**.

Upgrading Citrix License Server Monitoring

If you are upgrading from EdgeSight 5.3 and have been monitoring license servers running earlier versions of Citrix Licensing, you must upgrade to Citrix Licensing 11.9 to monitor those license servers with EdgeSight 5.4.

Upgrading Agents

Important:

- Perform the EdgeSight Server upgrade before upgrading the associated EdgeSight agents.
- Upgrading from a Technology Preview Release is not supported.

You can directly upgrade from the EdgeSight for XenApp 6 Agent 5.3 (64-bit) to the EdgeSight for XenApp 6 Agent 5.4 (64-bit). You can also directly upgrade from EdgeSight Agent 4.2 or 4.5 to EdgeSight Agent 5.4 using a new MSI file. If you do not have the latest service pack installed for a prior version, install the service packs for the specific version before upgrading to EdgeSight Agent 5.4. Agent data files (agent database and log files) and registry key settings are retained during the upgrade.

Important: If agents are not upgraded to a minimum version of 5.3, data for the associated device cannot be uploaded to an EdgeSight 5.4 server, as described in "Agent Requirements" in [System Requirements for EdgeSight 5.4](#).

Direct upgrades of EdgeSight 4.1 agents are not supported. If you are using an EdgeSight 4.1 agent, you can first upgrade to a 4.2 agent and then perform a 5.4 upgrade. This will retain agent data and settings. If you do not need to retain data, you can uninstall the 4.1 agent and reinstall an EdgeSight 5.4 agent.

Uninstalling Agents

You can uninstall an agent using any of the following methods:

- Execute the `msiexec` command for the EdgeSight MSI with the `/uninstall` argument.
- Right-click on **EdgeSight.msi** and choose **Uninstall** from the pop-up menu.
- Use the Add and Remove Programs feature on the Control Panel.

You may encounter an error during uninstallation indicating that files cannot be removed from the system. In most cases, clicking **Retry** will result in a successful uninstallation. After uninstalling an agent, reboot the target machine. If the machine is not rebooted, a subsequent attempt to install an agent will fail.

Note: The `DELETE_DATA_ON_UNINSTALL` property controls whether agent data files (agent database and log files) are deleted when the agent is uninstalled. The default setting is to delete agent data files. See [Installing EdgeSight Agents Using the Command](#)

[Line](#) for more information.

Upgrading EdgeSight in a Virtual Desktop Environment

The following upgrade information relates to upgrades from EdgeSight 5.0, 5.1, 5.2, or 5.3 agents to EdgeSight 5.4 agents:

- If you have existing EdgeSight Agents running on virtual desktops, you must uninstall and reinstall the agents.
- The Agent Database Server can be directly upgraded. Any agent databases currently resident on the server are also upgraded. This ensures that no data is lost when EdgeSight for Endpoints Agents are replaced with EdgeSight for Virtual Desktops Agents.

Because all required components must be in place, and because some installation steps are dependent on previous actions, the following task sequence is recommended:

1. Uninstall the agents.
2. Upgrade EdgeSight Server.
3. Upgrade the Agent Database Server ([Installing the Agent Database Server](#)).
4. Install the new agents ([Installing the Agent](#)).

Managing EdgeSight

EdgeSight Agents

The EdgeSight Agent is a service that runs on an end-user device, virtual desktop, or XenApp Server and collects data, which it writes into a client-side database. The agent collects data, aggregates the data into a payload, and sends the payload to the EdgeSight Server. The following types of agents are available.

- **EdgeSight for Endpoints Agent** - Endpoint agent software is designed for the user desktop or laptop environment. The agents operate continuously and discreetly on user systems collecting performance, resource, application and network data. The data is collected and stored in a local database and uploaded to an EdgeSight Server on a scheduled basis. Data can also be displayed directly from an agent database for use in problem resolution.
- **EdgeSight for Virtual Desktops Agent** - Virtual desktop agent software is designed to monitor virtual desktops based on XenDesktop 4.0 or later. In addition to monitoring system, application, and network performance, it collects ICA channel data including XenDesktop multi-media counters, collects end user experience metrics, and alerts on XenDesktop session performance. Note that this agent does not provide monitoring of the Desktop Delivery Controller (DDC).

Agents store data in a remote database and file share, with the EdgeSight Server acting as a database broker.

- **EdgeSight for XenApp Agent** - XenApp agent software is designed for use on XenApp Servers. Data is collected and stored in a local database and uploaded to an EdgeSight Server twice a day. Data can also be displayed directly from an agent database for use in problem resolution. There are two levels of EdgeSight for XenApp Agent:
 - *Basic* agents require only that you have a XenApp Enterprise license available on your Citrix License Server. The agent records information about client and server performance and application usage.
 - *Advanced* agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix License Server. The agent records information about user sessions, client and server performance, application usage, and network connections.

EdgeSight Server

The EdgeSight Server collects data from the distributed agents and allows administrators to display the data to identify potential issues in the enterprise and to assist in problem resolution. The following components make up the EdgeSight Server:

- **Web Server** - The web server component accepts the data uploads from the agents and then displays performance and availability information in a wide range of standard reports through the EdgeSight Server Console.
- **Database Server** - The database server component stores the data uploaded from the agents and acts as the data source for Reporting Services.
- **Report Server** - The report server component generates performance and availability information in the form of reports. The report server uses Microsoft SQL Server Reporting Services.

In an environment where EdgeSight for Endpoint Agents are monitoring virtual desktops in a pool, additional components are required:

- **EdgeSight Agent Database Server** - This provides data storage for agents running on virtual desktops in a pool. The EdgeSight Web Server includes database broker components from which agents acquire a connection to an agent database server. The database broker components are installed by default.
- **Agent data file share** - The agent data file share provides storage for files such as log files and INI files which are not stored on the EdgeSight Agent Database Server.

EdgeSight Server Console

Administrators interact with the EdgeSight Server through the EdgeSight Server Console. The console provides a powerful and flexible tool for displaying availability and performance information from the data collected by the distributed agents. To access the console, open a web browser to the URL for the EdgeSight Server and providing credentials on the logon page. An administrator can access the console using the following URL:

<http://servername/edgesight/app/default.aspx>

The EdgeSight Server Console has the following components.

- **Tabs** - Use the tabs at the top of the content area to select the type of data you want to display or operation you want to perform. Most of the information in this guide pertains to the Configuration tab. The tabs are as follows:
 - **Getting Started** - This tab provides overview information for each tab. Click on each tab name to display descriptions of tab features. A checkbox allows you to disable the display of this tab on your subsequent logins.
 - **Monitor** - This tab allows you to perform real-time monitoring of performance counters on specified devices and to display information on alert conditions.
 - **Troubleshoot** - This tab allows you to perform real time troubleshooting using troubleshooting tools and real time reports. The real time reports display data directly from an agent database.

- **Plan and Manage** - This tab allows you to display summary reports which provide an overview of your environment. Summary information can be displayed for devices, XenApp servers, users, processes, Websites, or transactions.
- **Track Usage** - This tab allows you to display reports on usage of Citrix licenses, on published application launches and users, and on session duration.
- **Browse** - This tab allows you to browse or search lists of reports and to display reports. You can also display report properties and subscriptions.
- **Configure** - This tab allows you to edit your user profile, configure companies (including agent options, alerts, devices, and security), configure the server (including licensing, authentication, database grooming, and company creation), and monitor server status (including messages, jobs, services, and agent database broker activity).
- **Menu Bar** - Use the Menu Bar at the top of the content area to perform common operations on the current page, such as adding a page to your list of favorites, refreshing a page, or printing a page. When displaying a report, you can add the report to the list of favorite reports or subscribe to the report.
- **Filter Bar** - Once a report is selected, use the Filter Bar to filter report data. Depending on the report selected, filter by department, group, time period, process, device, user, site, and other data types. Filter data to isolate information based on particular classes of processes, devices, or users and to quickly identify problems or trends. You can also filter data on non-report pages such as the Current Alert List or the administrative and configuration pages. Click Go to apply filter parameters.
- **Help Link** - Click the Help link at the top right of the console to invoke context-sensitive online help. In addition to context-sensitive help, the help system also provides reference material, such as a glossary of report metrics and a definition of SQL views.

License Server

Citrix Licensing 11.6 or later is used to supply licenses authorizing EdgeSight Agents to upload data to an EdgeSight Server. The license server can be anywhere on the network as long as it can be reached from the web server component of the EdgeSight Server and by the XenApp Agents. A single license server can be shared by multiple Citrix products, including multiple EdgeSight Servers.

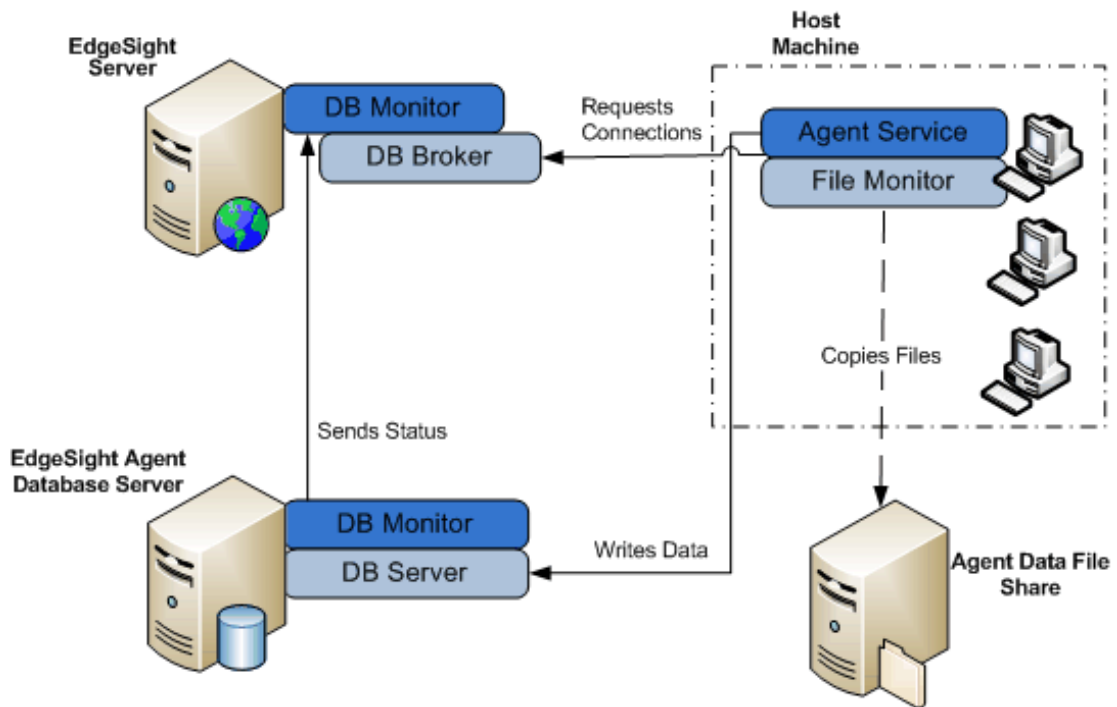
Note: The license server and the EdgeSight license files should be in place before deploying EdgeSight in order to avoid delays in uploading data.

Separate licenses for XenApp Agents and Endpoint Agents must be obtained, even if both types of agents are associated with the same server. All agent license files (for example, CESEP_*.lic) must be placed in the MyFiles folder of the license server directory on the EdgeSight Server.

For more information on EdgeSight for XenApp licensing, see <http://support.citrix.com/article/CTX126059>.

EdgeSight Components Required for Virtual Desktop Monitoring

When using EdgeSight to monitor virtual desktops where data is not persisted across reboots, additional components are required for storing agent data. The following figure shows the relationship between these components and the systems being monitored:



The components required for virtual desktop monitoring include the following:

- **EdgeSight Server** - Each EdgeSight Server installation includes database broker and database monitor components which supply database connection information to EdgeSight agents running on virtual desktops in a pool and listen for EdgeSight Agent Database Server registration and status.
- **EdgeSight Agent Database Servers** - The database servers store data collected by EdgeSight agents running on virtual desktops. The database monitor on each server communicates with EdgeSight Server to announce its availability and update status at regular intervals.
- **Agent Data File Share** - The file share stores agent files which are not stored in the EdgeSight Agent Database Server, such as log files and INI files.
- **EdgeSight Agents** - The EdgeSight Agents collect performance data for the virtual desktops or systems on which they are installed. During agent installation, you specify which EdgeSight Server is to supply database connection information and the path to the agent data file share.

The EdgeSight components function within a larger environment which includes Citrix Provisioning Server and may include XenServer.

For more information on using the EdgeSight Server Console to monitor the status of pools, agent database servers, and database broker messages, see [Displaying Agent Database Broker Status](#).

Terms and Concepts

A *company* is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies. Companies are broken down into *departments*. Departments are organized as a hierarchical tree with a default root department (All), and device-specific subdepartments (XenApp Farms, XenDesktop Farms, and Endpoints) which are created on installation. The structure of the XenApp Farms and XenDesktop Farms subdepartments is determined by the farms being monitored and cannot be changed using the EdgeSight Server Console. Additional Endpoint subdepartments can be created automatically as agents register with the server, or can be created manually. Configuration information is associated with agents based on their department. Each department corresponds to a set of systems running EdgeSight Agents. These systems are referred to as *devices*.

In addition to the department structure, you can organize devices by custom *groups*. A custom group is a user-defined collection of devices. Membership in a group can be based on the associated departments, device characteristics, or queries.

In addition to groups of devices, you can also create *user groups* which are collections of XenApp, XenDesktop, or endpoint users. Many reports containing data on user experience can be filtered by user groups, allowing you to monitor system performance for a group of users with specific characteristics.

EdgeSight Console *users* log on to the console to display reports or perform administrative tasks. (Note that reports use the term user to indicate a XenApp or XenDesktop user associated with a session.) Each console user is assigned a *role* (such as the default roles of Administrator or Report Viewer) which has an associated set of *permissions*. These permissions determine what actions a user can take and what pages are displayed on the console. For example, a user with a role of Report Viewer can display reports but cannot display pages under the Company Settings or Server Settings folders and perform administrative functions on the server.

Users can display reports from the console or can receive them based on a *subscription* which specifies the distribution of a report by email or to a file share. (This is an effective means of distributing targeted information to people in the organization without requiring them to log on to the console.) Subscriptions are distributed based on a defined schedule.

Agent Types and Processes

EdgeSight provides the following types of agents:

EdgeSight for Endpoints	Endpoint agents provide monitoring and data collection for physical endpoint devices.
EdgeSight for Virtual Desktops	Desktop agents provide monitoring and data collection for virtual desktops based on XenDesktop 4.0 or later.
EdgeSight for XenApp	<ul style="list-style-type: none">• Basic agents require only that you have a XenApp Enterprise license available on your Citrix License Server.• Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix License Server.

Agent Processes

The EdgeSight Agent includes the following key processes:

Citrix System Monitoring Agent Service	<ul style="list-style-type: none">• Collects data (resource usage, events, and hardware changes) from an end-user device, XenDesktop instance, or XenApp server.• Communicates with the EdgeSight Server on port 9035 for configuration downloads and payload uploads.• For an agent in a pooled desktop environment, requests a connection to a remote database.
Firebird Service process	<ul style="list-style-type: none">• Stores the data from the user device or XenApp server in the local agent database.
File Monitor process	<ul style="list-style-type: none">• Copies files to and retrieves files from an agent data file share, if an agent is installed on virtual desktops in a pooled environment.

The system overhead for the agent processes includes the following. Note that these are average values and may vary based on the individual machine and environment. (Note that agents installed on virtual desktops have smaller disk space requirements because they use a remote database for storage.)

- 1-2% CPU overhead
- 30-35 MB working memory
- 200 KB per day network utilization

- 40 to 250 MB of disk space

Agent Data Collection

Data collection is typically performed during hours of normal system usage to ensure that the data collected is an accurate representation of system availability and performance, without being skewed by large amounts of idle time. Some metrics, such as critical application and service resource statistics, are only collected when the user is actively using the system. The following types of data are collected and stored in the agent database:

- Performance data
- Event-driven data
- XenApp and XenDesktop data

Performance Data

Performance data includes polled data for system metrics, such as CPU or memory usage, that is a product of normal system operation. EdgeSight collects data including but not limited to the following:

- CPU utilization
 - CPU usage over a period of time
 - CPU comparisons on multiple devices
 - CPU utilization tracking
 - Which processes are consuming the most CPU
- Memory utilization
 - How much RAM is being consumed
 - Which applications are consuming the most memory
 - Which machines have the least free memory
- Disk utilization
 - How much hard drive space is available
 - Which systems have potential hard disk issues
 - Which machines have the least free disk space

Event-Driven Data

Event-driven data includes metrics that are generated by an event occurring on the user system, for example, when the user invokes and starts to use an application or when a socket connection is made. EdgeSight collects data including but not limited to the

following:

- Application issues (errors, crashes, and non-responsive applications)
 - What error message appeared
 - When the error occurred
 - How many times the error occurred
 - Which system generated the error
 - What else was running on the system at the time of the error
- Application usage (especially useful for tracking license compliance)
 - How long was the application running in memory
 - How much active or idle time has elapsed
 - What applications are being used by which users
- Network connection
 - Response time for network communications
 - Average speed of the network
 - Amount of network volume being utilized
 - Round trip time for certain connections
 - Systems experiencing the most delay
 - Applications generating the most volume
 - Slowest responding servers
 - Protocols in use on the network
 - Sites visited and new sites

XenApp and XenDesktop Data

XenApp data includes, but is not limited to, the following:

- End User Experience Monitoring (EUEM) data, including session performance, ICA round trip, and client and server startup metrics. This ICA round trip data replaces the session latency data collected by older agents.
- Session activity, such as active, inactive, and total sessions
- Session auto-reconnects
- ICA session input and output bandwidth for audio, video, printers, and file operations
- IMA service state and availability

- Resource usage, such as memory and CPU, for groups of users
- Session network delay and round trip time for groups of users
- Published application launches and unique users, by farm or by user group
- Active Application Monitoring data, such as application test response times and application test failures

XenDesktop data includes, but is not limited to, the following:

- ICA channel data including XenDesktop multi-media counters
- End User Experience metrics
- XenDesktop session performance

Agent Data Aggregation

Agent data is aggregated in the following way:

- Data is collected and then stored every 5 or 15 seconds in the local agent database. Endpoint data is stored every 5 seconds, and XenApp data every 15 seconds.
- Every twenty minutes, the collected data is aggregated into 5 minute increments and placed in a new location in the local agent database.
- Once a day, the 5 minute increments are re-aggregated into one hour increments and then uploaded to the EdgeSight Server based on the configured upload schedule.
- Data is stored for 3 days in the agent database so that historical information can be displayed. After 3 days, the data is groomed from the agent database; however, the time that the data is retained can be extended by editing the agent properties.

If the agent software is installed on a mobile device, or the device is unable to connect to the EdgeSight Server, aggregated data is retained for up to 5 days for XenApp servers and 29 days for endpoints and virtual desktops, or until the device is able to upload to the server. You can configure the data retention time as required. For more information, see the Agent Properties Wizard topic in online help.

Agent Data Upload

When the agent is first installed, it registers itself with the server and obtains information about when data is scheduled to be uploaded to the server and what data is required by the server.

Using the default Performance Upload worker configuration, data is uploaded from the agent database to the EdgeSight Server. Endpoint agents upload once a day by default, XenApp agents upload twice a day, and Virtual Desktop agents upload every hour and a half. You can configure agents to upload more frequently if required. For instance, a mid-day data upload can be scheduled to evaluate morning activity. For more information on worker configurations, see [Configuring, Scheduling, and Running Workers](#).

A typical data upload size for an EdgeSight for Endpoints agent is 80KB. EdgeSight for XenApp agent data uploads are typically larger due to the greater amount of data collected and can reach 300KB. These data upload sizes depend on a number of factors such as the agent properties and the usage profile of the system hosting the agent.

The data upload process can be summarized as follows:

1. The EdgeSight Agent contacts the EdgeSight Server to find out what data is requested based on when the last successful upload occurred.
2. The agent queries the local database and aggregates the polled payload data into one-hour increments.
3. The payload data is compressed and sent to the web server components of the EdgeSight Server using either HTTP or HTTPS. (HTTPS is used if the agent is configured to connect to the server using SSL. SSL support must be enabled on the server, and a valid SSL certificate issued by a trusted certificate authority must be present on the server running the EdgeSight Website.)
4. The payload data is stored in the local data folder from where it is retrieved and processed by the EdgeSight Script Host (RSSH).

Administrative Tasks and Roadmap

In order to perform administration tasks, you must be assigned the Administrator role or you must have been granted administrative privileges. Administrative tasks are grouped at the company level and the server level.

In order for an administrator to view and edit server-wide settings, they must be granted the Manage Server Settings permission. This permission is automatically granted to the Superuser created during installation. For additional users, it must be explicitly granted when the user is created or edited rather than by role assignment.

Company settings only affect a single company, while server settings affect all companies resident on the server. Company settings include both server and agent settings.

When you perform the initial configuration of EdgeSight using the Post-Installation Wizard, you explicitly specify a number of critical operating parameters for EdgeSight Server. These include an initial (or root) company, a Superuser account that can access all companies on a server and can create new users, email settings used to send server notifications, and a port for use in communication with the license server. In addition to these explicitly set parameters, there are many default settings which enable EdgeSight to be fully operational as quickly as possible. This section outlines the remaining tasks that you perform after installation and initial configuration to reach full operational status. Some of these tasks differ depending on your environment, such as the type of systems being monitored and whether you are using the default email authentication provider or Active Directory for authenticating users.

Configure Authentication for Reporting Services

Microsoft SQL Server Reporting Services must be installed and configured in order to generate and display EdgeSight reports. Once EdgeSight is installed, you must configure credentials used to authenticate the EdgeSight Server to the Report Server. For more information, see [Configuring Reporting Services](#).

Add Roles

Before adding users (people who can log on to the EdgeSight Server Console), it is recommended that you add any roles that will be required to determine what actions they can perform on the console. For more information on defining roles, see “Creating Users and Assigning Roles” in [Managing Roles](#).

Add Authentication Provider

If you want to automatically create users based on an Active Directory tree, you must add an AD authentication provider. Before creating a new provider, make sure you have the LDAP path for your AD authentication provider available. For more information on adding an AD authentication provider, see [Managing Authentication Providers](#).

Add Users

If you are using the default email authentication provider, you can add users and assign roles to them from the EdgeSight Server Console. For more information, see “Creating Users and Assigning Roles” in [Managing Roles](#).

Adjust Agent and Worker Configurations

Depending on your environment, you may need to adjust which agent and worker configurations are applied to the devices in a department. Default agent and worker configurations are supplied for endpoint, XenApp, and virtual desktop systems. Verifying that devices are in the correct departments and that the appropriate agent and worker configurations are applied to these departments helps ensure efficient EdgeSight Server operation. It is recommended that you use the default configurations for a period of time and then adjust the configurations if required to resolve data collection issues. For more information on agent properties, see [Setting Agent Properties](#). For more information on worker configurations, see [Configuring, Scheduling, and Running Workers](#).

Managing Company Settings

Company settings allow you to manage the configuration of companies hosted on a Citrix EdgeSight server. All company settings are located on the Configure tab under the Company Configuration menu item.

Company settings allow you to perform the following tasks:

- Managing User Profiles
- Managing Company Properties
- Managing Departments, Devices, and Groups
- Managing User Groups
- Managing Roles
- Creating Users and Assigning Roles
- Managing Access to XenApp Farms
- Creating Alert Rules and Actions
- Managing Application Categories and Vendors
- Managing Reports
- Managing IP Ranges
- Managing Real-Time Dashboard Configurations
- Setting Agent Properties
- Configuring, Scheduling, and Running Workers

Managing User Profiles

Each EdgeSight Server Console user has a profile stored on the server which includes name, title, and contact information. Users can edit their own profiles. Click on **My Settings > Profile** to display the profile matching the username under which you logged in to the console.

You can display the profiles of other EdgeSight Server Console users on the Users page (**Company Configuration > Security > Users**). For more information on the creating and managing users, see "Creating Users and Assigning Roles" in [Managing Roles](#).

Managing Company Properties

A company is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies. If there are multiple companies on the server, use the Company drop-down menu at the top right hand corner of the console to switch between companies. Company settings are administered separately from server settings, allowing server administrators to control which users are authorized to display reports or change settings for a specific company. To display company settings, navigate to **Company Configuration > Settings**.

Time Zone and Daylight Savings Time

There is a time zone for each company on an EdgeSight Server. The time zone is used by the server when displaying times in reports, when scheduling and running maintenance jobs, and for timestamps associated with events, such as alerts and upload times. All data for a company is consolidated based on the day boundary for that time zone. This ensures greater data consistency when agent machines are in a number of different time zones. In addition to the time zone setting, you can specify whether or not to adjust times for Daylight Saving Time.

When EdgeSight is installed, an initial company must be created, including a time zone setting. The Company Settings page allows you to change the company time zone as required. When creating new companies using the console, you must specify a time zone.

Agent Registration Settings

Agent registration settings control how EdgeSight Agents make themselves known to the server. (Agents initiate communication with the server in all cases except for explicit requests for agent data, as in the case of displaying a real time report from the console.) Use the menus to enable or disable each setting, then click **Save Changes** to apply the new settings. Enabling all the client registration settings is recommended. Allowing EdgeSight software to handle agent registration, department creation, and duplicate instances can save you time and effort that would otherwise be spent on manually resolving these events. The following table describes how each setting affects client registration.

Registration Setting	Controls...
Automatically Register Agents	When an agent connects to a server, it passes Company and Department configuration information. If this information matches an existing company defined on the server and this setting is enabled, then the agent is enlisted into the company. Otherwise, the agent is an unmanaged instance and only appears on the Unmanaged Devices page. (For more information on moving unmanaged devices to a company and department, see Handling Unmanaged Devices .)

Automatically Create Departments	When an agent connects to a server, it passes Company and Department information. If the Department does not exist, then it will be created if this setting is enabled. If the setting is not enabled, the device is placed in the root department for the company. (For more information on departments, see Managing Departments, Devices, and Groups.)
Coalesce Duplicate Instances	<p>If an EdgeSight Agent database becomes corrupt, as part of the repair process the machine will be matched up with its historical data on the server if this setting is enabled. If the feature is disabled, then there will be a duplicate record of the device in the system. You are notified of the creation of a duplicate record by a message on the Messages page similar to the following:</p> <pre>EdgeSight - New Instance (DUPLICATE) - Machine: 'sysname' Domain: 'domain_name'</pre> <p>An internal identifier (a globally unique identifier or GUID), rather than the machine name, is used to match duplicate instances.</p>

Managing Departments, Devices, and Groups

Companies are broken down into departments. Departments are organized as a hierarchical tree with a default root department (All), and device-specific subdepartments (XenApp Farms, XenDesktop Farms, and Endpoints) which are created on installation. Endpoint subdepartments which can be created automatically as agents register with the server, or created manually by a user with administrative privileges. Each department corresponds to a set of devices (systems running EdgeSight Agents).

In addition to the department structure, you can organize devices by custom groups. A group is a user-defined collection of devices. Membership in a group can be based on the associated departments, device characteristics, or queries.

Managing Departments

The root department (named All by default) and the XenApp Farms, XenDesktop Farms, and Endpoints subdepartments are created during the installation of EdgeSight. You cannot delete these default departments. The root department uses the Endpoint default configuration for agent properties and agent workers. Alert rules must be explicitly associated with the root department. The structure of the XenApp Farm subdepartment is determined by the XenApp Farm structure, and the structure of the XenDesktop Farm is determined by the Desktop Delivery Controller. These subdepartment structures cannot be changed using the EdgeSight Server Console.

Endpoint subdepartments can be automatically created based on information from agents as they register with the server. When an endpoint agent connects to a server, it supplies Company and Department information. If the Department does not exist, then it will be created if the Automatically Create Departments setting is enabled, as described in “Agent Registration Settings” in [Managing Company Properties](#). If the setting is not enabled, the device is placed in the root department for the company.

Use the Department page to create, edit, or delete endpoint subdepartments and also to associate alert rules and configuration settings with devices in the department. Alert rules, worker configurations, and agent properties can be created or edited any time, but they are not used until explicitly associated with departments. See “Departments” in the console online help for detailed instructions on creating and editing departments and mapping rules and configurations to departments.

Managing Devices

The devices displayed on the Devices page represent systems which are running EdgeSight Agents and have successfully registered with the server. Devices can be XenApp servers, desktops, laptops, or terminal servers. They can also be physical or virtual machines. If you have selected the default agent registration settings, which allow automatic agent registration and department hierarchy creation, the list of devices is automatically populated with all agents configured to communicate with the server. Once an agent running on a device has registered with the server, you can move the device to another department as required. (See “Agent Registration Settings” in [Managing Company Properties](#) for more information on agent registration.)

The device name, domain, and last upload time for the device are always displayed. The remaining device information can be selected using the **Show** drop-down menu. Refer to online help for a complete list of information available. Note that the last upload time shown in the Devices table is the last time a payload from that device was processed by the server. This is a useful indicator that agents are properly uploading data to the server.

If a specific device does not appear on the list, this may indicate a problem with company/department assignment. Navigate to **Server Configuration > Unmanaged Devices** to display a list of devices which have registered with the server, but are not associated with a company or department.

Creating and Using Custom Groups of Devices

You can create custom groups of devices on EdgeSight Server. Groups are collections of devices based on departments, a selected set of individual devices, SQL queries, or a combination of these criteria. When EdgeSight is installed, several commonly used groups are provided, such as “Citrix XenApp” and “All Windows Server 2003.” A group can be defined using one or more of the following criteria:

- All of the devices in one or more departments
- A selected set of individual devices within a department or across departments
- A selected set of individual devices to be excluded from the group
- A set of individual devices selected using an SQL query run against the EdgeSight database

Groups allow you to isolate and display data based on specific device characteristics, helping you to resolve cross-department system management issues. The following examples illustrate cases where custom groups are useful:

- You are asked to evaluate the performance enhancements to be realized from moving to a new operating system. Create custom groups of devices based on the devices running the current and new operating systems and compare group performance over time.
- You are asked to determine the effectiveness of a software patch prior to enterprise-wide deployment. Create custom groups of devices with and without the patch installed and compare the performance and availability of the target application over time.

- You are asked to closely monitor a group of devices at risk of problems due to known hardware issues. These devices reside in several different departments. Create a custom group of target systems and filter incoming alerts using the group.

Groups have the following attributes:

- **Name**—A unique name identifying the group. The name should be descriptive enough to allow a console user to readily select the correct group from a drop-down menu.
- **Expiration period**—A selected time period after which the group expires and is deleted. This feature facilitates the management of groups created for short-term projects with a set duration, such as the evaluation of software. Groups can also be set to never expire. No explicit notification is sent before group expiration.
- **Refresh period**—A selected time interval after which the device cache for the group is refreshed. Device cache refreshing ensures that devices which meet the criteria for group membership are detected and added to the group.
- **Public/Private**—Groups can be public (available for use by all console users who have a role of Administrator) or private (available only to the user who created the group). Private groups for a subset of all console users are not currently available.
- **Member Type**—Groups can be populated based on one or more of the following criteria: department, a selected set of devices, or an SQL query. Departments can be included as a single department or as a department tree, which includes the selected department and all subdepartments. A set of devices can be selected from a list of existing devices or imported from a comma separated value (CSV) file. Basing groups on an SQL query is an advanced capability that will probably only be necessary in certain cases where you require a set of devices based on a narrow set of criteria. In these cases, you will need to use database tools to expose the database structure.

Note: It is good practice to set the expiration period to a value which reflects the lifetime of the related task. For example, if you are evaluating a patch and need to collect 3 weeks of data, choose 1 month as the expiration period. If you need additional time to collect data, you can always edit the expiration period. Setting realistic expiration periods helps keep the list of groups manageable for you and for other users (if the groups are public). In addition, because the group's device cache is refreshed at regular intervals, setting expiration periods helps manage system resources wisely.

For detailed instructions on creating custom groups, see the “Groups” topic in online help.

Managing User Groups

In addition to groups of devices, you can also create groups of users. The user group capabilities of EdgeSight enable you to create collections of users by selecting users by username, IP address or IP range, or by running a SQL query against the EdgeSight database. The users can be XenApp, XenDesktop, or endpoint users. Many reports containing data on user experience can be filtered by user groups, allowing you to monitor system performance for a group of users with specific characteristics.

To manage user groups, go to **Company Configuration > User Groups**. User groups have the following settings: name, public/private setting and members. User groups can be public (available for use by all console users who have a role of Administrator) or private (available only to the user who created the group).

Members can be explicitly selected from a list of users (identified by user name or by IP address), selected based on a range of IP addresses, or selected based on a SQL query run against the EdgeSight database. Note that when a user group cache is updated, if the group membership is controlled by a query, the query is rerun and any new users matching the query will be added to the user group. This greatly simplifies the maintenance of query-based groups. For detailed instructions on creating user groups, see the “User Groups” topic in online help.

Managing Roles

When users are configured on a Citrix EdgeSight Server, they are assigned one or more roles. Roles define a set of permissions which control what operations a user can perform. An EdgeSight Administrator can define new roles and edit existing custom roles. There are two non-editable system-defined roles, Administrator and Report Viewer. The Administrator role has all permissions and the Report Viewer has a limited set of permissions that enables the user to view all EdgeSight reports. Creating a role involves selecting the permissions associated with the role. Optionally you can assign the roles to existing users. For more information on creating roles, see the "Add New Role" topic in online help.

Creating Users and Assigning Roles

A user is an individual (or group of individuals) for which an account is created on the EdgeSight Server Console. When the initial server configuration is performed, a Superuser account is created. This account has access to all companies hosted on the server and can create other users. The Superuser can create an account for one or more administrators for a company, and then the administrators can continue with the creation of additional user accounts as required. You create and manage users on the Users page (**Company Configuration > Security > Users**). After you create a user, an email is sent to the user which includes login instructions and a temporary password. For detailed instructions on creating users, see the "Users" topic in online help.

User access to the EdgeSight Server Console is controlled through login authentication, while a user's capabilities to display and edit data and perform administrative operations are controlled by a system of roles and permissions.

User logons are authenticated by either the built-in EdgeSight provider (user email address and password) or Active Directory (AD). (See [Managing Authentication Providers](#) and the "Authentication" topic in online help for information on creating an AD authentication provider.)

New users can be assigned one of the built-in roles (Administrator or Report Viewer) or assigned a previously created custom role. Each role is defined by a set of permissions. Assigning a role to a user automatically grants the associated permissions to that user. For detailed instructions on creating roles, see the "Roles" topic in online help.

To display the full set of permissions which can be assigned using a role, navigate to **Company Configuration > Security > Roles**, click on the information icon for the Administrator role, and then select the **Permissions** tab in the detail pane.

Note that the Manage Server Settings permission does not appear on the list. This permission must be explicitly granted when a user is created or edited rather than granted by role. While other permissions allow users to perform operations at the company level, this permission allows a user to view server-wide settings.

Managing Access to XenApp Farms

Use the Farm Authentication page to create and maintain default credentials used in accessing XenApp farms. The credentials consist of a farm name, user name, password, and domain name. The credentials are used when querying farms directly while searching for active sessions. (The report is accessible from the **Troubleshooting** tab.)

To find user sessions and display this report, you must select a query method. The **Query one or more farms directly** method is the recommended method for locating an active session for a specific user. Because this method requires existing credentials for logging in to the selected farms, you must specify a set of credentials for each farm in order for reports to be generated based on this query method.

Note: Credentials cannot be saved for a department which has no devices.

Creating Alert Rules and Actions

This topic outlines basic real-time alert concepts and provides strategies and guidelines for implementing alert rules in EdgeSight. For detailed instructions on creating real time alerts and actions, see the “Alert Rules” and “Alert Actions” topics in online help.

Real-time alerts allow you to monitor mission-critical applications and devices and notify designated people in your enterprise in the event of a problem. By default, alert data and statistics are collected by the agent on each desktop and uploaded to the server on a daily basis. When you explicitly configure an alert by creating an alert rule, you are requesting real-time notification that a specific alert condition has occurred.

The purpose of real-time alerts is to provide timely notification of critical events that require immediate attention. For example, alert rules ensure that data is available for display in the Farm Monitor. The Farm Monitor allows you to browse through a XenApp Farm and display real-time alerts and system context for one or more devices. When developing an alert rule strategy, ensure that alert rules are only created for events that have an associated resolution. Real-time alerts are not intended for data collection; agents collect relevant data whether or not an alert rule exists, and historical reports are the most effective means of displaying availability and performance data.

Proper alert configuration is critical to effective real-time alert notification on the health of distributed devices and applications. It enables you to quickly identify which issues are truly critical and require immediate attention and which issues can wait. In order to achieve an effective alert configuration, you must have an alert strategy in place. When designing your strategy, you will need to do the following:

- **Identify which applications are critical to your business or service** - Focus on critical applications and define alerts only for problems that must be resolved in a short period of time.
- **Identify which departments have mission-critical applications running on their systems** - Associate alerts only with the departments or groups where the alert condition is most critical. This allows you to isolate and respond to problems that are relevant to a specific portion of your business.
- **Identify which alert types are most important** - Some alerts, such as NT log alerts, are generated in large numbers by some applications and are generally transparent to the end user. As a result, prior to defining an NT log alert, verify the risk level of the alert condition by examining historical alert reports.
- **Identify what response is required to resolve specific alerts** - Responses may include performing a specific set of actions or notifying responsible individuals in the associated department. If no response can be identified for a condition, the event does not require a real-time alert.
- **Identify who is responsible for responding to the alert** - Determine who should respond to a specific alert condition.
- **Establish and publish guidelines for alert rule creation** - Determine who is responsible for new alert rule creation. Define best practices, such as creating descriptive names

for alert rules and avoiding duplicate alert rules. A user must have the Manage Alerts permission in order to create or edit an alert rule.

Once you have established an alert strategy, you can configure the required real-time alerts using the Alert Rules page in the EdgeSight Server Console (**Company Configuration > Alerts > Rules**).

Alert Features

A number of features enhance the ability to configure alert rules specific to a condition warranting an alert, and thus reduce the number of extraneous alerts generated by the agent. These precise alert rules should result in an actionable response if the alert is ever generated. The following is a list of some of the improved scenarios:

- Performance alert rules can be specified on complex parameters. For example, send a System Performance alert if the CPU is over x% and there is less than y free memory on the machine.
- Application alert rules can be defined to specify the company name of the process from which to generate alert rules. For example, if a process written by the specified company crashes, send a Process Fault alert to the company's internal support team.
- Windows Event Log alert rules can be specified to include the application and event writing the event to the event log. For example, if a group policy violation occurs, send an alert to the Security team.
- Negation logic (implemented as a **Not like** checkbox) can now be used in the definition of certain alert rules. For example, send an application terminated alert notification only if the terminated process was not written by the Internal Tools Team.

Alert Categories and Types

Real-time alerts can be broken down into two distinct categories: event driven and polled. Event driven alerts are generated whenever the associated event occurs in the system, while polled alerts are based on queries of the agent database on a periodic basis. In general, polled alerts are used as notifications of performance problems with an application, a system, or the network. For a description of how polled alerts function, see "Sampling, Polling, and Re-alerting Parameters" later in this topic.

When setting up alert rules using the Alert Rules Wizard, alerts are grouped into the following types based on the type of event or condition with which they are associated:

- Application alerts
- System alerts
- Network alerts
- XenApp performance alerts
- XenApp error alerts

- Session performance alerts
- XenDesktop error alerts

To help ensure that real-time alert data is available for XenApp Servers, the following alerts are preconfigured and assigned to the XenApp Farms subdepartment:

- Configuration Logging Database Unavailable
- Farm Data Store Connection Failure
- Health Monitoring and Recovery Action Failure
- Health Monitoring and Recovery Test Failure
- IMA Service is Unresponsive
- License Server Connection Failure
- Number of Servers in a Zone is Too High
- Published Application Concurrent Usage Limit
- Session in Down State
- Terminal Server Client Connection Error
- Terminal Server License Server Discovery Failure
- Zone Data Collector Election Triggered
- Zone Elections Too Frequent

The parameters for these alerts can be edited. Descriptions of each alert rule and parameter set is provided in the Alerts Rule Creation Wizard.

Active Application Monitoring Alerts

The EdgeSight Server Console displays real-time alerts received from Citrix Active Application Monitoring (AAM) software. This software allows you to record and create virtual user scripts and define tests. When the tests are run, virtual user ICA sessions are generated on the target XenApp servers. The results of the tests provide application response and availability information.

Important: The EdgeSight for XenApp Agent 5.0 or later running in Advanced Mode is required for the generation of Active Application Monitoring alerts.

The Active Application Monitoring alert rules are as follows:

- The Application Response Failure alert is generated when a monitored transaction has failed.
- The Application Response Time alert is generated when the time to execute a monitored transaction has exceeded the specified threshold.

These alerts are grouped under XenApp Performance alerts. For more information on installing the software, see [Install and Configure](#). For more information on creating and launching tests, see the online help included with the Active Application Monitoring software.

Notes on Specific Alerts

The following information on specific alerts is provided to help you understand under what conditions these types of alerts are triggered.

- **New process alert** -The new process alert only fires for processes which are used for the first time after the New Process Grace Period has expired. The grace period is set in the agent properties (for more information, see [Setting Agent Properties](#)). For example, the default grace period on XenApp agents is 7 days. If you install an agent and then start a process, the agent records this as a process, but not as a new process because the agent database is less than 7 days old. Once the database is more than 7 days old, then any new process (any process that is not already in the agent database) being run will trigger an alert. This avoids a large group of alerts being triggered at once because an agent was installed. Note that the grace period is relative to the agent database age, not the actual date of initial agent installation. If an agent database is recreated for some reason, then the grace period is reset.
- **Process hung alert** - This alert type corresponds to the “not responding” alerts shown in reports. EdgeSight software uses the Windows API (the `IsHangAppWindow` call) to determine if an application is not responding. An application is considered to be not responding if it is not waiting for input, is not in startup processing, and has not called the `PeekMessage` function within the internal timeout period of 5000 milliseconds (5 seconds).
- **Process fault and process snapshot alerts** - These types of alerts may generate crash reports, if conditions on the managed device allow for crash data to be captured. In some cases, the system is unable to support the collection of data. In the case of process fault alerts and the resulting crash reports, there are several factors to consider:
 - If the crash file cannot be written, a message to that effect is logged to the `zcrash_loader` log file. Navigate to **Server Status > Server Script Host**, locate `es_zcrash_loader`, click on the menu icon and select **View Log**.
 - What is the age of the crash report? Crash report grooming is distinct from database grooming, and the time that crash reports are retained is controlled by the **Max Keep Days** setting. Navigate to **Server Configuration > Settings** and select the **Crash Processing** tab.
 - What is the limit for number of logs collected, and how much space is allocated to crash reports? (See **Server Configuration > Settings**.) If either the maximum number of crash logs or the maximum disk consumption limit is exceeded, application crash processing is disabled until the limit is increased. There is no reset operation that can be used to remove existing payloads.
- **Published Application Single Use Failure and Published Application Concurrent Usage Limit** - When enabling logging of connection control events on the XenApp server, the **Log over-the-limit denials** setting must be enabled to allow these SMA-based alerts to fire. (For XenApp 6 systems, use the **Logging of logon limit events policy** setting.) See the [XenDesktop](#) documentation for more information about configuring connection control events.

Sampling, Polling, and Re-alerting Parameters

Sampling is the periodic collection of data from the system being monitored. *Polling* is when the agent runs a query against the database to compare alert rule parameters to the data collected.

Each rule for a polled alert includes the following parameters:

- Percent of samples required
- Poll interval
- Re-alert

Most polled alert rules also include a non-editable Data sample window parameter, usually set to Poll interval plus one minute.

These parameters allow you to fine tune the frequency with which alerts of a specific type can be triggered. Sampling is performed as frequently as every 5 seconds, depending on the alert type. During sampling, the required data for the alert type is collected. When polling occurs, the collected data is compared to the conditions specified in the alert rule. The poll interval value determines how often polling is performed. The percent of samples required determines what percentage of the collected samples must be across the threshold (either higher or lower depending on the alert type) before an alert is triggered. If the alert defined by the alert rule has already been triggered within the re-alert period, another alert is not generated until the period expires and the alert condition reoccurs. The data sample window indicates how far back in time samples are included in the polling.

Note: The default poll interval is designed to provide timely generation of alerts while minimizing the impact of queries run against the database. Decreasing the poll interval (increasing the frequency with which queries are run) can have an adverse effect on system performance and should be done with caution.

Polled Alert Example

The following illustration shows an alert rule for detecting system slowdowns due to high CPU usage.

Rule Type:	System Slowdown
Rule Name:	System slowdown due to high CPU time
Standard Parameters	
• CPU time (percent)	40
• Processor queue length	
Advanced Parameters	
• Data sample window	Poll interval plus one minute
• Percent of samples required	10
• Poll interval	90 seconds
• Re-alert	Every poll interval

The alert functions as follows:

- EdgeSight Agent software samples the percentage of CPU time used. For the purposes of this example, the sampling rate is assumed to be every 5 seconds.
- Every 90 seconds, the software polls the sampled data to see if the percentage of CPU time has exceeded 40 percent in at least 10 percent of the total number of samples. Because the data sample window is defined as the poll interval (90 seconds) plus one minute (60 seconds), the samples gathered over the last 150 seconds are included. This means that 30 samples will have been gathered. If 3 or more samples out of 30 have a percentage of CPU time used over 40, an alert is generated.
- The re-alert parameter is set to **Every poll interval**, so if the percentage of CPU time exceeds the threshold in the data included in the next polling, another alert is generated.

When to Configure a Real-Time Alert Rule

EdgeSight does not require that you configure certain alert types for the EdgeSight Agent to collect data on the conditions which would generate the alert. If you are configuring an alert rule, you should only do so if you are in a position to respond to the alert within a matter of hours. If there is no appropriate response to the alert condition within several hours from alert generation, a historical report should be used to determine if an item of significance has occurred. Creating excessive numbers of alert rules can reduce the effectiveness of monitoring tools such as the Farm Monitor by flooding it with alerts, making it more difficult to identify truly critical events.

Performance Impact of Real-Time Alerts

Regardless of the alert rule type, there is some processing overhead for each rule configured for an agent. At a minimum, the agent must determine if the alert should be generated, and if so, it must send the alert to the server. In some cases, the agent must run an SQL query against the database to determine if alertable conditions are present; when the conditions are too broad, the agent is required to process large datasets to generate the alerts and send them to the server.

Since each alert rule configured for a given agent incurs processing overhead, and this processing may occur when the end-user is attempting to perform an important task, care should be taken to only configure alert rules which are both targeted and actionable. If there are concerns about the overall impact of the agent on a system, and a significant number of alert rules have been defined for that agent, you may want to reevaluate the defined rules to determine whether a historical report would be more appropriate than real-time alerts. The following list provides some general guidelines as to when a set of alert rules will negatively impact the end user:

- If more than 3 or 4 application or network performance alerts are defined.
- If process or network performance alerts are defined to trigger for common conditions, such as CPU usage over 5%.
- If process or network performance alerts are defined for very complex conditions (for example, populating a value for more than 2 or 3 performance thresholds). In these cases, the SQL queries run by the agent to determine if an alertable condition exists could themselves consume significant database cycles.
- If “Not Like” is defined on process or network performance alerts.
- If multiple textual “Like” or “Not Like” operations are defined on process or network performance alerts.
- If performance alert rules are defined which will never fire (for example, setting up a process performance alert for an application whose execution is blocked via group policy).

When Will the Server Show a Real-Time Alert?

Real-time alerts are not generated until the following conditions are met:

- Alert rules are created and assigned to a department.
- Devices have run the Init Worker or the Configuration Check Worker.
- The condition or event specified in the alert rule has occurred.

Note: Some XenApp alert rules are preconfigured and assigned to the XenApp Farms department as described in “Alert Categories and Types” earlier in this topic.

No alerts of any type are sent to the server until the agent has completed its startup sequence, which may take several minutes. Init and Configuration Check workers are run after the startup sequence completes, and worker execution is spaced out over several

minutes. Once an alert is generated, it is batched for delivery to the server. Alerts are batched for up to one minute, and assuming there is a network connection, sent to the server. If there is no network connection, or if the agent is stopped before the alerts can be sent, the queued alerts will not be received by the server, and will not be re-sent. (Real-time alerts are not guaranteed to be received by the server.) However, because the agent does not require real-time alerts to be configured for data collection, the alert condition is still captured and can be seen in the historical reports once a data upload occurs, even though they were not sent to the server as real-time alerts. Unsent alerts are also shown in the real-time alert reports that display data directly from the agent database.

Managing Alert Actions

The Alert Actions page (**Company Configuration > Alerts > Actions**) allows you to configure an alert action to be performed when a specific alert condition occurs. Alert actions can be used to:

- Send an email message.
- Generate an SNMP trap.
- Launch an external executable process on the EdgeSight Server.
- Forward alert data for Microsoft System Center Operation Manager (SCOM). For information on integrating EdgeSight alert actions with SCOM, see [Integrating EdgeSight Alerts with Microsoft System Center Operations Manager](#).

A single action may be associated with multiple alert rules. For example, there are multiple cases where an IT manager should be notified in case of an alert condition, so an action resulting in an email message being sent to the manager is associated with each applicable alert rule.

Note: Although only an EXE file can be launched using the “Launch an external executable process” alert action, you can launch cmd.exe and use command line arguments to call a non-EXE file such as a BAT or VBS file.

For information on creating alert actions, see the “Alert Actions” topic in online help.

Managing AlertSuppressions

The Alert Suppressions page (**Company Configuration > Alerts > Suppressions**) displays alerts that have been suppressed. As an administrator, you can edit or clear any alert suppression.

Any user can create an alert suppression from the Alert List located on the **Monitor** tab. Suppressions prevent the EdgeSight Server Console from displaying a specific type of alert based on source, device, or user, or by a combination of these criteria. Note that suppressions are only effective for the user creating them; other users are still able to view the alerts. For more information on alert suppressions, see the “Current Alert List” and “Alert Suppressions” topics in online help.

Managing Application Categories and Vendors

EdgeSight includes extensive application category and vendor listings for use in reporting by type of application or by software manufacturer. In many cases, the program fits into an existing category and matches an existing vendor. If necessary, you can create a new category or a new vendor for the new process. See the “Edit Categories” and “Edit Vendors” topics in online help for detailed procedures for creating and editing categories and vendors.

Managing Reports

EdgeSight provides a wide range of standard reports. These reports are available once EdgeSight Server has been installed and the connection to Reporting Services has been configured.

Managing Report Subscriptions

A subscription is a standing request to distribute a report in a selected format at specified times. Report distribution (subscription type) is done by email or by transfer of a file to a file share. Subscriptions can be public or private. Public subscriptions are displayed on the **Subscriptions** tab of the report details pane. Private subscriptions are only displayed to the subscription creator or an administrator. A subscription is a useful method of distributing targeted data to people in your organization without having to give them access to the EdgeSight Server Console. To display existing public subscriptions, navigate to **My Settings > Subscriptions**.

You can create a subscription while viewing the report using the **Subscribe** link in the filter bar. You can also create a subscription from any report list by displaying report properties and selecting the **New Subscription** button from the **Subscriptions** tab. See “Working with Reports” in online help for a detailed procedure for creating subscriptions.

By default, as an administrator, you are granted the required permissions to manage all subscriptions, both public and private. (See “Creating Users and Assigning Roles” in [Managing Roles](#) for descriptions of permissions and their relationship to roles.) This allocation of permissions allows you to control the distribution of data within your organization and also help you manage the impact on the Report Server.

Uploading Reports

Navigate to the Custom Reports page (**My Settings > Custom Reports**) and click on the **Upload a Report** button to transfer an RDL file for a custom report to the Report Server.

Always use a unique name when uploading a new report. Also, you should define and publish naming conventions for custom reports. Use the **Public** or **Private** radio buttons to determine whether the report is shared within your company. Public reports are displayed to all users unless the ability to view the report is restricted based on the selected permissions. Private reports are only displayed to the user uploading the report. The Public/Private attributes cannot be changed once the report is uploaded. To change any of these attributes, you must delete the report and then upload the report again.

If you make additional changes to the report, use the **Update** link on the Properties page to upload the RDL (Report Definition Language) file. For more information, see the “Custom Reports” and “Upload Custom Reports” topics in online help.

Managing IP Ranges

Setting IP ranges enables you to define the corporate network for use in filtering the network by corporate or external network hosts. Ranges of IP addresses defined on this page are represented as corporate network sites. This option is only required when the IP address you use is not defined in the private, non-external IP address range. For instructions on setting IP ranges, see the “IP Ranges” topic in online help.

Managing Real-Time Dashboard Configurations

EdgeSight provides a dashboard that allows you to display real-time information for specific devices and counters, based on a saved configuration. The dashboard is displayed on the **Monitor** tab.

Note: Devices must be running an EdgeSight Agent of version 4.2 or later in order to be displayed on the dashboard.

The Real Time Configurations page allows you to create and edit named configurations for the dashboard. Configurations include:

- A unique name
- Timeouts for queries and connections
- An update interval
- Counters to display for the selected devices

You can select a maximum of 20 devices and 8 counters for the configuration. See the "Real Time Configurations" topic in the online help for detailed instructions on creating and editing configurations.

Once a configuration has been created, it is added to the drop-down menu on the Dashboard page, allowing users to select the configuration for viewing on the dashboard. The dashboard is populated with data based on direct queries to managed devices; no dashboard data is stored on the server.

Setting Agent Properties

The EdgeSight Agent stores configuration data in two locations. The Windows registry on the managed device is used to store configuration items which are machine specific and are required for successful communication with the EdgeSight Server. For example, the name of the company the agent belongs to, the name of the server to contact, and any proxy information required to perform the communication are all stored in the registry. All other configuration items are stored in the EdgeSight Agent database. When the agent is running on virtual desktops in a pooled environment, the agent database is located on a remote server.

The items stored in the Windows registry are typically set once, and are supplied during agent installation. All other configuration items are supplied by the associated EdgeSight Server, and any changes in configuration are performed using the Agent Properties page. By default, an agent obtains its initial configuration shortly after the agent first runs and then queries for configuration changes. The default schedule for configuration checks is set to 6:30 AM agent local time every day for endpoint devices and every hour for XenApp servers. Agents running on virtual desktops in a pooled environment will perform configuration checks based on actual usage.

Care should be taken when changing agent properties. These parameters control the way the agent works and could result in users perceiving data loss or an increased CPU usage by the agent. In most cases, you will not need to customize agent properties. Use the default configuration at first and adjust it over time based on user requirements and system performance.

Agent property configurations are displayed on the Agent Properties page (**Company Configuration > Agents > Properties**). When creating a new set of agent properties, you must choose a default configuration (Endpoints Default, XenApp Default, or Virtual Desktop Default) to use as a template. Provide a unique configuration name and description, and edit the parameters as required.

Note: If you have performed an upgrade from an EdgeSight Server version prior to 5.0 SP2, the Virtual Desktop Default configuration is not initially displayed in the list of agent property configurations. To create agent property settings for virtual desktops, select **New Properties Configuration** and then select the **Default Properties for Virtual Desktop Agents** radio button. Configure the properties as described in the “Agent Properties Wizard” topic in online help.

Once a custom set of agent properties has been created, it must be explicitly mapped to a department before it is provided to agents as part of a configuration check. (See “Managing Departments” in [Managing Departments, Devices, and Groups](#) for information on associating a set of agent properties with a department.)

For information on the individual parameters that make up agent properties, see the “Agent Properties Wizard” topic in online help.

Minimal Data Collection Mode

In order to support busy XenApp server environments, the EdgeSight agent has a Minimal Data Collection Mode feature that, when enabled, limits the data collected on the agent and thus the overall impact the agent has on the XenApp server.

When a XenApp server is consistently experiencing heavy load, or the XenApp server slows considerably under load, it is time to consider using this feature. Use EdgeSight reports to note the number of sessions and processes at which a considerable slow down occurs. These numbers are used to establish when Minimal Data Collection Mode is initiated on the agent.

Note: Minimal Data Collection Mode should be considered a temporary measure to ensure that critical data is collected while long term measures are taken to reduce or redistribute the load on the affected XenApp servers.

The Minimal Data Collection Mode is disabled by default. To enable it, edit the agent properties and display the advanced settings. Set **Manage Data Collection** to True and enter values that you collected in the **Process Count Threshold** and **Session Count Threshold** fields. Then assign this set of agent properties to the XenApp server experiencing the problem.

When Minimal Data Collection Mode is enabled, the agent periodically monitors the process and session counts against the configured thresholds. If either threshold exceeds its specified value, the agent enters Minimal Data Collection Mode. At this point an operational alert is sent to the server, “The Citrix System Monitoring Agent has entered Minimal Data Collection Mode.” When both process and session counts return below the threshold settings for 5 minutes, the agent will leave Minimal Data Collection Mode and normal data collection will be resumed. A bullet is sent to the server to indicate that the agent has left Minimal Data Collection Mode.

Minimal Data Collection differs from normal data collection in the following ways:

- No module data is collected or persisted
- No network data is collected or persisted
- No light trace events are persisted
- No image or principal events are persisted (currently not visible)
- No task details used in fault reports will be persisted
- Hung application detection is disabled
- Image and session performance data is persisted at a 2 minute granularity
- Custom performance counter collection is disabled
- Performance, network, and event trace alerts are disabled

Other configuration changes that exist on EdgeSight for XenApp include:

- System, image, and session performance fine grain data is persisted at 15 second intervals.

If the scheduler detects more than 5 concurrent sessions running, it will not use idleness to gate when scheduled items such as consolidation can run. Instead the assumption is made that this is a server system and therefore there may never be best idle moments for schedules to run.

Individual workers can be configured on the server to similarly ignore idleness when making a determination for a best time to run.

Configuring, Scheduling, and Running Workers

Workers are tasks that run on EdgeSight Agents. Default worker configurations and schedules are created during EdgeSight Server installation. You cannot edit or delete default configurations and schedules, but you can use them as templates using the Copy operation and then editing the parameters as required.

Although workers are scheduled to run at certain times, the actual execution of workers takes into account when a user is actively using the system. If possible, workers are run when the system is idle. See “Configuring Workers” later in this topic for more information scheduling workers.

As with agents configurations, care should be taken when changing worker configuration parameters. These parameters control when and how often workers are run and could result in users perceiving increased CPU usage by the agent. In most cases, you will not need to create custom worker configurations. Use the default configuration at first and adjust it over time based on user requirements and system performance.

Once a custom worker configuration has been created, it must be explicitly mapped to a department before it is provided to agents as part of a configuration check. (See “Managing Departments” in [Managing Departments, Devices, and Groups](#) for information on associating worker configurations with departments.)

The EdgeSight workers that you can configure are as follows:

- **Asset History**—Collects the asset history for managed devices. This worker can be disabled.
- **Configuration Check**—Checks for configuration changes to be downloaded to managed devices from the server.
- **Database Maintenance**—Performs database maintenance tasks on the agent database.
- **Drive Space Calculation**—Calculates the drive space used on managed devices. This worker can be disabled.
- **Fault Report Cleanup**—Maintains and cleans up files created for fault and snapshot reports.
- **Performance Upload**—Uploads agent data to the EdgeSight Server.

Configuring Workers

A worker configuration has the following components:

- A configuration name and description—The name and description should be complete enough to allow administrators to accurately select a configuration.

- A set of enabled workers—Only the Asset History and Drive Space Calculation workers can be disabled. All other workers are required to run for proper system operation.
- A set of run conditions—In addition to the worker schedule, a set of run conditions is used to control the behavior of the worker.
- One or more schedules—Each enabled worker must have at least one schedule configured that, along with the run conditions, determines when the worker is run.

The run conditions for workers are as follows. Not all run conditions are set for each worker.

- **Days before the worker will force itself to run**—This setting indicates that the worker will run after the specified number of days, even if other conditions (such as user idle time) are not met. If the worker can not run due to communications problems, it will run as soon as communications are restored.
- **Randomize the start with a window of**—To facilitate system and network performance, worker execution times can be randomized within a time window. This prevents situations such as a large number of agents attempting to upload performance data at the same time.
- **Consider system idle after all users are idle for**—This setting helps to run workers when users are not actively using systems. (The worker schedule has a similar option called **Wait until all users are idle before starting the worker**.)

Note that a run condition must contain a non-zero value to be enabled. Entering zero as the value for a run condition automatically disables that condition. For more information on configuring workers, see the “Workers Configuration Wizard” topic in online help.

Monitoring Workers

Some workers log information into log files. The SYS_EVENT_TXT.txt file indicates which workers have run and at what time. It is located by default in your installation path:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data` for Microsoft Vista and Windows 2008 systems

`%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data` for all other systems

For agents running on virtual desktops in a pool, the log files are copied to an agent data file share specified during agent installation.

It also logs any errors that may occur when a specific worker tries to run, which is helpful when diagnosing issues. Not all workers create a log file, however, because they are internal to the product and provide product maintenance. The following lists group the workers by the type of task they perform:

Workers that interact with the server:

- worker 101: Performance Upload—uploads Agent data to the EdgeSight server

- worker 104: Init Worker—runs on the initial database creation, connects to the server, and downloads initial agent property information
- worker 105: Configuration Check—checks for configuration changes
- worker 109: Trace Route Worker—executes a network trace
- worker 150: Bullet Worker—uploads alert information to the EdgeSight Server

Workers that collect data:

- worker 102: Drive Space Calculation—calculates drive space on the device
- worker 103: Asset History—collects the asset history of the device

Workers that maintain the agent:

- worker 1: Database Tuning—internal maintenance, no log is created
- worker 2: Database maintenance—internal maintenance, no log is created
- worker 106: AD Worker—runs an Active Directory script
- worker 107: Fault Report Cleanup—maintains and cleans up files created for fault and snapshot reports
- worker 108: Fault Report Preparation—builds fault reports and uploads them to the server
- worker 110: RISH Log Cleanup—maintains and cleans up logs created from RISH
- worker 126: Database Sizing—database size tuning

You may also see other logs different than the ones described above in this directory. This is because some alerts run as scripts and log their activities.

The worker log files contain information that can be useful in troubleshooting issues that can occur relating to the various work functions performed by the agent. You would first look in the `SYS_EVENT_TXT.txt` file to see if a worker has experienced any issues. Based on the information there, you would then look to the specific worker log for more detailed information.

For example, if the `SYS_EVENT_TXT.txt` file makes a reference to the following error message:

```
Running worker 101 - 'Performance Upload' with trigger 1071
```

Then you would look in the log folder for the text file that begins with `Worker101_Trigger1071`.

The most useful logs tend to be the ones associated with the upload and configuration workers, as they help to resolve connectivity issues between the agent and server. For that reason, the logs for workers 101, 104, and 105 are typically the most useful in troubleshooting these sorts of problems. For example, you can verify that agent communication with the server is failing if you examine the `SYS_EVENT_TXT` file, locate Worker 104 running with trigger 24 and see a status of anything other than 0x0.

License Server Monitoring

If desired, you can use the License Server Monitoring feature of EdgeSight 5.4 to monitor license servers that are running Citrix Licensing 11.9. All related settings are located on the **Configure** tab under the **License Monitor Configuration** menu item.

Note: You can monitor earlier versions of Citrix Licensing (11.5, 11.6, or 11.6.1) by setting up a separate EdgeSight Server running EdgeSight 5.3.

License server monitoring does not depend on an EdgeSight Agent to gather information. Once a license server has been configured for monitoring, EdgeSight Server directly polls the license server for information on license usage. Polling is performed by the `core_lsm_license_poller` server script. The data returned from the license servers is displayed in the Citrix Licensing reports available from the **Track Usage** tab.

Note: If there is a firewall between the Citrix License Server and the EdgeSight Server, you must specify a static Citrix Vendor Daemon Port number on the license server. Refer to your Citrix License Server documentation for more information.

Managing License Server Polling

Use the Settings page to configure how often the specified license servers will be polled and if email is to be sent to the EdgeSight Administrator if polling fails. The timer controlling when polling occurs starts after the previous polling cycle is completed. For example, setting the polling interval to 15 minutes means that a polling cycle will be initiated 15 minutes from the time that the last polling cycle completed. To assist you in selecting a reasonable poll interval, the total time taken to poll all configured license servers is displayed.

As you add more license servers, or network traffic increases, you may need to increase the poll interval to ensure that all servers are polled within the polling interval. Similarly, if you decrease the number of license servers, you may want to reduce the polling interval and retrieve license data more often.

The order in which license servers are polled can change from one polling cycle to the next, because EdgeSight starts by polling the license server which has not been polled for the greatest amount of time. For more information on polling settings, see the “Add or Edit License Server Configuration” topic in online help.

Configuring License Servers for Monitoring

The License Servers page allows you to configure which license servers are to be monitored, enable and disable polling for a server, and delete a server configuration. Once you configure a server and enable polling, the license server is polled in the upcoming polling cycle.

You may want to disable polling for a server if polling errors are occurring and the problem is being investigated, or if the server is being taken down for upgrade or maintenance. Previously collected license information from disabled servers will still appear in the License Usage Trending report, but no new license information is displayed for the disabled server in the License Usage Summary report.

Important: Deleting a license server configuration deletes all license usage data associated with that license server from the EdgeSight database. After deletion, no data from the license server is displayed in the license usage reports.

For more information on configuring license server monitoring see the “License Servers” and “Add License Server Configuration” topics in online help.

Managing Server Settings

Server settings allow you to manage global settings on a Citrix EdgeSight Server. All server settings are located on the **Configure** tab under Server Configuration and Server Status. Server settings allow you to perform the following tasks:

- Monitoring Server Status
- Configuring Server Settings
- Creating Companies
- Configuring Data Uploading
- Managing Licenses
- Managing Authentication Providers
- Configuring the Connection to Reporting Services
- Managing Reporting Services Schedules
- Managing the Database
- Handling Unmanaged Devices
- Displaying Agent Database Broker Status
- Displaying and Responding to Server Messages
- Managing Server Scripts

Monitoring Server Status

The Status page (**Server Configuration > Status**) provides you with an overview of server operations across all companies. The Company table lists how many devices have and have not uploaded data to the server during the current day, by company. It also lists how many new devices running EdgeSight Agent have registered with the server for the current day and during the previous week. The status for messages, unmanaged devices, alerts, and crash reports simply provide a count indicating activity for the current day.

Status Type	For detailed information...
Company	Navigate to Company Configuration > Device Management > Devices to display details on when specific devices uploaded data to the server and to display information on new devices.
Server Script Host	Click Server Script Host Status to display the Server Script Host Status page. Navigate to Server Configuration > Settings and select the applicable tab to display and manage settings for Data Upload and Crash Processing.
Message Status	Click Message Status to display the most recent messages.
Unmanaged Devices	Click Unmanaged Devices to display information on unmanaged devices. An unmanaged device is a system with an EdgeSight Agent installed that is not associated with a company and department.
Alerts	Select the Monitor tab and then select either Alert Console or Alert List to display information about the most recent alert notifications.
Crash Reports	Select the Monitor tab and then select Alert List and filter for Process fault or Process snapshot alerts. See the <i>Citrix EdgeSight User's Guide</i> for more information on accessing and using crash reports.

Configuring Server Settings

The Settings page (**Company Configuration > Settings**) allows you to control how EdgeSight Server handles the following capabilities:

- Agent Support and License Server
- Agent Database Broker Logging
- Notifications
- Timeouts
- Data Uploading
- Application Crash Processing
- SSL Support
- SNMP Port

In most cases, you will not need to adjust any of the values or settings on this page. We recommend that you use the default settings and observe server performance in production conditions before considering the adjustment of server settings.

Agent Support and License Server

Depending on the Citrix EdgeSight products installed in your environment, you may want to enable or disable the display of reports displaying data from XenApp servers or from endpoints. You may also want to select the level of support offered for EdgeSight for XenApp agents: Basic or Advanced.

- *Basic* agents require only that you have a XenApp Enterprise license available on your Citrix License Server. The agent records information about client and server performance and application usage.
- *Advanced* agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix License Server. The agent records information about user sessions, client and server performance, application usage, and network connections.

This setting only determines whether reports and administrative pages are displayed on the console; data continues to be collected, uploaded, and stored even if display support is disabled. Note that unlike alert suppression settings, this is a server wide setting and affects what all users see when using the console. For more information on what tools and reports are displayed based on agent type, see [EdgeSight Feature Availability](#).

To enable or disable support, choose an option from the support drop-down menus. If you select an option which excludes available data from being displayed, such as disabling XenApp agent support for a server which has EdgeSight for XenApp agents reporting up to it, a confirmation box is displayed.

If EdgeSight for Endpoints support is enabled, you can also edit the name and port of the Citrix License Server which supplies licenses for endpoint systems.

Agent Database Broker Logging

This **Agent Database Broker** tab allows you to enable the display of detailed broker log messages. This option is set to Off by default. If this option is enabled, additional status messages are displayed on the Broker History page. (See “Displaying Broker History” under [Displaying Agent Database Broker Status](#) for more information.) Detailed logging always occurs on the agent database broker; this feature simply controls the display of data on the Broker History page. This feature is useful for providing detailed information when debugging agent database broker issues.

Notifications

The SMTP server name and email addresses are specified during server installation, but can be changed as required.

Important: It is critical to server operation that a valid SMTP server name is used. EdgeSight Server uses the SMTP server for many features, including the distribution of alert notifications, server error conditions, and new user passwords.

The following table defines the notification options. The email options enable the server to send email to the EdgeSight Administrator Email Address in the event of agent or server errors.

Option	Definition
New Agents	This option is recommended as an effective means of notifying an administrator by email that new devices will be uploading data to the server. Client registration is controlled by company-specific settings as described in Managing Company Properties .
Agent Errors	You may want to enable this option when first using Citrix EdgeSight Server to help detect and resolve agent property issues. This option may not be necessary once these issues have been resolved. In most cases, agents are able to automatically recover from errors.
Server Errors	You may want to enable this option when first using Citrix EdgeSight Server to help detect and resolve configuration issues. This option may not be necessary once these issues have been resolved.
Communication Errors	This option is recommended as an effective means of alerting an administrator to device communications problems.

Send an email when there is bad HTTP read of a payload (not recommended)	This option is not recommended for normal use because uploading of payloads is retried as required. You may want to enable this option for use in debugging a specific problem uploading payloads.
Attach Payload	This option is not recommended for normal use because uploading of payloads is retried as required. This option may not be necessary once these issues have been resolved.

Timeouts

Timeouts are specified for common server operations (such as database queries and ASP page loading, data upload queries, and background service queries) to prevent the server from being blocked while waiting for a response to a query. We recommend that you use the default values unless a specific problem occurs with excessive timeouts.

Note that the Farm Monitor and Alert Console (located on the **Monitor** Tab) use the ASP.NET Page and Query timeout when performing queries for alert data. If you experience frequent timeouts when using these pages, increase the ASP.NET Page and Query timeout as required.

Data Uploading

Data uploading refers to the collection of queued database payloads from machines running an EdgeSight Agent. In most cases, the default values are sufficient for proper operation. Values may need to be adjusted if you receive repeated messages warning of too many queued payloads or other data upload issues. Note that the minimum CPU, memory, and active time timeouts are intended to ensure that only data from machines with more than a minimal amount of activity is uploaded to the server. This provides an accurate view of availability and performance data across the company.

Application Crash Processing

Because application crash logs can be large files, the capability is provided to limit the retention of crash logs by number, by disk consumption, and by date. These limits help prevent crash logs from consuming too much space on the server. You can also disable application crash processing, in which case, no crash log files are uploaded to the server.

If either the maximum number of crash logs or the maximum disk consumption limit is exceeded, application crash processing is automatically disabled until the limit is increased. There is no reset operation that can be used to remove existing payloads.

SSL Support

The SSL Support feature enables secure logins. A valid SSL certificate issued by a trusted certificate authority must be present on the server running the EdgeSight Website. If SSL support is enabled, all agent to server communications must be over SSL. If an agent attempts to connect to an SSL-enabled server without using SSL, an error is generated. Any attempts to establish a connection to the agent (such as running a worker remotely or displaying a real time report) will display an error stating that SSL is required, but this connection did not occur over SSL.

SNMP

The SNMP Trap Port to be used for outgoing SNMP trap alert actions. This port setting is used for all SNMP trap alert actions defined for all companies hosted on the server. EdgeSight allows you to set the port so that you can avoid conflicts with other management tools which may be using the default SNMP outgoing port. For more information on creating SNMP trap alert actions, see [Creating Alert Rules and Actions](#).

Creating Companies

A company is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies. You create an initial company when installing EdgeSight Server. After installation and post-installation configuration is complete, navigate to **Server Configuration > Companies** to create additional companies as required.

The only information required for creating a company is a name and a time zone. Company names must be unique on the server. If you have multiple EdgeSight Servers and intend to create reports across servers, ensure that the company name is unique on all the servers.

The time zone is used by the server when displaying time stamps and triggering jobs. There is a single time zone for each company defined on an EdgeSight Server. All data for that company is aggregated based on the day boundary for that time zone. This ensures data consistency when agent machines are in a number of different time zones.

Managing Licenses

This section describes how to manage EdgeSight licenses. For information on configuring EdgeSight to monitor Citrix License Servers, see [License Server Monitoring](#).

Citrix Licensing supplies licenses authorizing EdgeSight Agents to upload data to an EdgeSight Server. The license server can be anywhere on the network as long as it can be reached from the EdgeSight Web server and by EdgeSight for XenApp agents. A single license server can be shared by multiple Citrix products, including multiple EdgeSight Servers. It is highly recommended that the license server and EdgeSight for Endpoints license files be in place before completing the initial configuration of EdgeSight.

Important: You must obtain separate licenses for EdgeSight for Endpoints and EdgeSight for XenApp agents, even if both types of agents are associated with the same server.

The EdgeSight for Endpoint agent license file (for example, CESEP_*.lic) is located in the MyFiles folder of the license server directory, for example:
%ProgramFiles%\Citrix\Licensing\MyFiles.

For more information on EdgeSight for XenApp licensing, see <http://support.citrix.com/article/CTX126059>.

Configuring Licensing for EdgeSight for Endpoints Agents

If EdgeSight for Endpoints support is enabled, you are required to enter a license server name and port during EdgeSight Server installation. During initial configuration using the Post-Installation Wizard, you can test the connection to the license server and, if successful, display the type and number of licenses installed.

EdgeSight Server obtains licenses on behalf of EdgeSight for Endpoints agents from the specified server. You can change the license server name and port after installation by navigating to **Server Configuration > Settings** and editing the **License Server Name** and **License Server Port** fields as described in “Agent Support and License Server” in [Configuring Server Settings](#). The current license server name and port are displayed on the Licensing page, as described in “Using the Licensing Page to Monitor License Status” later in this topic.

Configuring Licensing for EdgeSight for XenApp Agents

After EdgeSight for XenApp Agents are installed, they receive default agent properties from the associated EdgeSight Server. These properties instruct the agent which license server should be contacted to obtain a license. The following license server options are available:

- XenApp—Use the same license server as the XenApp server on which the agent resides. This is the default setting in the XenApp Default agent properties.

- Farm—Use the XenApp Farm’s license server.
- Custom—Use an explicitly defined license server and port.

For more information on agent properties, see [Setting Agent Properties](#) and the “Agent Properties Wizard” topic in online help. As with any agent properties, these settings apply to entire departments and are inherited by sub-departments unless overridden at a lower department level.

EdgeSight for Endpoint Agent Licensing

For EdgeSight for Endpoint Agents, licensing works as follows:

- During post-install configuration, you can validate the connection from the EdgeSight Server to the license server. This is optional, and the post-installation wizard can complete without a valid license or connection.
- The license file installed on the license server specifies the number of EdgeSight for Endpoints agents allowed to upload data to the server.
- EdgeSight Server regularly contacts the license server to determine if sufficient licenses are available. If the license server detects that only a few EdgeSight for Endpoints licenses remain, a warning message is sent to the EdgeSight Server.
- If the number of agents specified in the license is exceeded, agents are not allowed to upload data to the server. Data collection continues and data is retained in the agent database until groomed.

The EdgeSight Server requires one license for each endpoint device reporting up to it. At server startup, the EdgeSight Server attempts to check out one license for each existing device. If not enough licenses are available for the existing devices, all available licenses are checked out and allocated to agents based on when the agent first uploaded data to the server; older agents are given licensing preference over newer agents. Only licensed agents are allowed to upload data to the server. (Devices running agents are tagged as licensed or not licensed in the EdgeSight database.) The server retries license checkouts every minute when it is unable to acquire licenses for all agents. A warning message is added to the messages table and an email is sent to the server administrator. To remedy a shortage of licenses, you must install new licenses, or delete existing devices until compliance is reached.

Once the server is able to properly start up, when a new device reports up to the server, the server checks out a license for that device. After the server has secured a license for a given device, that device can always upload, and further license checks are not performed (except for the startup case mentioned above). If a new endpoint agent is unable to upload due to a license shortage, data collection continues and data is retained in the agent database until groomed. As with the startup case, you must install new licenses, or delete existing devices until compliance is reached before the new devices can upload data.

When a device is deleted from a server, the license for that device is checked in to the license server and available for use by another device.

“Server startup” actually refers to the Server Script Handler (RSSH) startup. When RSSH is stopped, all licenses checked out for that server are checked-in, and available for use by other servers using the same license server, until RSSH restarts. This is important to

remember when planning for the number of licenses required. If you have an insufficient number of licenses to cover all devices across all servers, another EdgeSight Server could check out licenses causing a license shortage at startup.

EdgeSight for XenApp Agent Licensing

For EdgeSight for XenApp Agents, licensing works as follows:

- EdgeSight for XenApp Agents communicate directly with the license server to obtain a license for each session. Agents checkout a license as part of session start on the XenApp server
- If a license is not available, a breach is logged (notifying EdgeSight Server of a problem), but data collection continues for the session. If a user starts more than one session on a XenApp server, or sessions across servers, the same license is used across sessions (as with XenApp licenses).
- The number of license violations is allowed to exceed the value specified in the license, but excess uploads are blocked after 5 days of license violations occur during the license monitoring period. (Multiple license overages on a single day count as a single violation). Excess uploads are blocked and discarded until no more breaches occur for a specified time period or the license is upgraded.
- To help ease installation and configuration, the initial data upload from a XenApp server is not checked for license violation. Any violations in the initial payload are ignored and discarded.

Important: An EdgeSight for XenApp Agent will attempt to monitor all sessions on that XenApp server and cannot monitor only a portion of sessions on the system. In other words, if you purchase EdgeSight for XenApp for a portion of your concurrent user (CCU) base, you need to understand the approximate session load on a given server and then determine how many servers must have the agent deployed to handle the load. Take this information into account when determining license requirements.

Using the Licensing Page to Monitor License Status

Use the Licensing page (**Server Configuration > EdgeSight Licensing**) to display current license usage and status information. The Licensing page displays the following information:

EdgeSight for XenApp License Statistics

<p>Current Licensing Status</p>	<p>Indicates whether the system is in compliance with the license. In compliance indicates that the number of allowed license violation days have not been exceeded. The license status can be one of the following:</p> <p>In Compliance—All of the existing devices reporting to this server were able to acquire licenses.</p> <p>Warning—The number of licenses used has exceeded the number of licenses allowed during this monitoring period. See the Violation Days field for the number of violation days and the servers reporting the violations.</p> <p>In Violation—The number of licenses used has exceeded the number of licenses allowed for at least 5 days during this monitoring period.</p>
<p>New Device Grace Period</p>	<p>During this period, agents reporting up with licence violations will not have payloads rejected. A warning email is sent to the EdgeSight Administrator, and a message is posted to the Messages page, indicating that a license violation has occurred. This feature allows administrators to fix problems with initial configurations.</p>
<p>Allowed Violation Days</p>	<p>The number of days during the monitoring period for which the number of licenses used are allowed to exceed the number of licenses granted. Uploads are blocked if the number of violation days in the monitored period exceeds five (5) days.</p>
<p>Violation Monitoring Period</p>	<p>The number of days for which license violations are tracked.</p>
<p>Violation Days</p>	<p>The current number of days during the monitoring period for which the number of licenses exceeded the number of licenses granted. Expand this item to display the dates of license violation and the names of the servers reporting the violation.</p>
<p>Endpoint License Statistics</p>	

<p>Current Licensing Status</p>	<p>Indicates whether the system is in compliance with the license. The license status can be one of the following:</p> <p>In Compliance—The EdgeSight Server was able to acquire licenses for all of the existing devices reporting to this server.</p> <p>Error—The EdgeSight Server was unable to acquire licenses for all of the existing devices on this server. EdgeSight will continually attempt to acquire licenses for all devices.</p> <p>Stopped—The License Manager is not currently running.</p> <p>You may also see a message informing you that the server is in the process of acquiring licenses. If, on startup, the server is unable to acquire licenses for all registered endpoint devices, a message is displayed and the server retires license acquisition every 15 minutes. You can retry immediately by clicking the Refresh Endpoint Licensing button. This button is only displayed if there is a license acquisition failure on startup.</p>
<p>Licensed Devices on This Server</p>	<p>The number of endpoint licenses currently in use by agents reporting to this server. This is displayed in terms of the total number of agents registered with the server. For example, if there are 500 agents registered with the server, and 487 agents are currently using licenses, this field would display 487 of 500.</p>
<p>License Server</p>	<p>The license server name and port number from which EdgeSight obtains endpoint agent licenses. The server and port are specified during installation and can be changed after installation on the Settings page.</p>
<p>Total Installed Licenses</p>	<p>The total number of endpoint agent licenses specified by the installed license file.</p>
<p>Available Licenses</p>	<p>The number of licenses available for use by endpoint agents.</p>
<p>Expiration Date</p>	<p>The date at which the license file will expire. You will be notified prior to license file expiration.</p>

Managing Authentication Providers

Authentication providers ensure that only authorized users can log on to an EdgeSight Server. The first step in creating a new user is to select an authentication provider against which a username and password are verified.

A default authentication provider (Email) is included when you install EdgeSight Server. You cannot edit or delete the default authentication provider. The default authentication provider uses an email address as the username. When you create a new user, you specify the email address for the user. Then, an email is sent to the user explaining the sign in process and providing a temporary password. When the user first logs on, they are requested to change their password.

You can create new authentication providers that use Active Directory (AD) for security and sign-on capabilities. Before creating a new provider, make sure you have the LDAP path for your AD authentication provider available.

To set up Active Directory integration with EdgeSight, you must set up an Active Directory authentication provider: Before you begin, make sure you have the LDAP path for your authentication provider available.

1. Log into the EdgeSight Server Console.
2. Navigate to **Server Configuration > Authentication** in the navigation pane to display the Authentication Configuration page. Note that the Email provider is already listed.
3. Click the **New Provider** button to invoke the Authentication Provider Wizard.
4. Click **Help** and follow the instructions provided in the Authentication Provider Wizard topic.

Setting Up Users and/or Groups

Once you have added an authentication provider and set up roles, you must also set up users and/or groups. You may want to create multiple groups within your Active Directory, such as an EdgeSight Admin Group, and an EdgeSight Console User Group for ease of Administration.

1. Navigate to **Company Configuration > Security > Users** in the navigation pane to display the Manage Users page.
2. Click the **New User** button to display the User wizard.
3. Click **Help** and follow the instructions provided in the Add User Wizard topic.
4. Test the new user or group setup. Log out of the EdgeSight Server and log in again. At the Login page, the **Provider** drop-down menu is now displayed. The user or group member selects the applicable provider and then logs in using their domain user ID and password.

Configuring Reporting Services

Configuring the Connection to Reporting Services

Microsoft SQL Server Reporting Services must be installed and configured in order to generate and display EdgeSight reports. For detailed installation and configuration procedures for Reporting Services and related software, see *Configuring Reporting Services for Citrix EdgeSight*.

After the Reporting Services installation and configuration is complete, you must configure the connection from EdgeSight Server to the Report Server. Navigate to **Server Configuration > Reporting Services > Report Server** to specify the report server, credentials for accessing the report server and the data source, and default report and schedule operations. For more information, see the “Report Server Settings” topic in online help.

Managing Reporting Services Schedules

Reporting Services schedules, in conjunction with the subscription feature, allow you to automate the generation of reports for distribution to users. When an administrator or a user creates a report subscription, they must select an associated schedule. Navigate to **Server Configuration > Reporting Services > Schedules** to manage existing schedules and create new schedules. For more information, see the “Reporting Services Schedules” topic in online help.

In some cases, such as a week with a holiday or a scheduled company shutdown, you may want to pause report schedules so that the associated reports are not generated.

Care should be taken when deleting schedules. If the deleted schedule is associated with a report, the report will not be generated. Also, subscriptions using the deleted schedule will not result in a report distribution.

Managing the Database

You can manage the size of the EdgeSight database by configuring what data is uploaded from agents to the server and how long data is retained before being groomed. These tasks can help ensure acceptable database performance.

Configuring Data Uploading

You can select what types of performance and availability data you want to upload to the server (**Server Configuration > Data Maintenance > Upload Configuration**). This allows you to optimize EdgeSight Server performance by limiting data uploads to reflect the data used in your enterprise.

The uploading of XenApp Environmental Usage data is disabled by default, and should only be enabled if you plan to use the Environmental Usage report, which displays this data. Depending on the number of sessions for the group or device, the data used to generate these reports can significantly increase the size of your EdgeSight database. In many cases, you may want to enable data collection for a period of time as required and then disable data collection when no longer needed.

Database Grooming

EdgeSight collects a wide range of performance, availability, and usage data about end-user systems, applications, user sessions, and the network. The EdgeSight Agents collect data from systems and upload it to a EdgeSight Server. Depending on the number of endpoint and XenApp systems, the number of applications, and network activity, databases can grow quickly without proper management. The primary database management mechanism is grooming.

Grooming is the process of removing older data from a database at regular intervals to make room for new data. Grooming is critical for maintaining efficient database operation. An effective grooming schedule controls database size and helps ensure acceptable performance while retaining sufficient data for business operations.

The following example shows how database grooming settings affect the size of the EdgeSight Server database. You have deployed EdgeSight agents on 2500 end user devices. The devices are running an average of 50 processes and visit an average of 100 Websites over the period of time that network data is retained. The agents are collecting data for 12 hours each workday. Changing the grooming parameter for Network Statistics from 7 to 14 days increases the size of the database by about 40 percent, roughly equivalent in its effect on database size to adding 1000 devices.

Grooming Schedule

EdgeSight has a distributed structure, with EdgeSight Agent databases on each managed device which are uploaded to a single EdgeSight Server database. The data retention

settings for the agent database are specified as part of the agent properties and are applied to devices based on their department membership. If persistent data upload timeouts occur for agents using the same configuration, you may want to consider decreasing the values for the Days To Keep In DB and Max Days To Keep In DB agent configuration settings. In some cases, this may result in a loss of data, especially if managed devices are unable to connect to the EdgeSight Server.

The grooming schedule for the server database is specified as part of the server configuration. The server grooming schedule allows you to specify the number of days that data is retained by data type. This allows data used to identify trends, such as performance data, to be retained longer than data which quickly becomes stale, such as real-time alert data.

The default values for grooming the server database are sufficient for most installations. You may want to use the default values at first and adjust them over time based on user requirements and system performance. In cases where you want to retain more data, consider creating an archive report or performing data warehousing as methods of keeping historical data in preference to relaxing the grooming configuration. See the *Citrix EdgeSight User's Guide* for more information on using EdgeSight data for analysis and record keeping.

Server Database Grooming

Navigate to **Server Configuration > Data Maintenance > Grooming** to edit the database grooming schedule, as described in the “Grooming Configuration” online help topic. The Grooming table contains the following information:

- Report Data—The type of data to be groomed.
- SQL Server Table—The database table where the data is stored.
- SQL Server View—The SQL views associated with the database table where the data is stored. These views are used in modifying reports and creating custom reports. Online help includes definitions of all views.
- Groom Days—The default number of days that data of the selected type is retained before grooming is performed.

In most cases, the grooming schedule is configured to retain one month of data. Application usage data is retained for 90 days due to the need in many environments to track application usage for license and compliance reporting. On the other hand, network data is only retained for 10 days due to high data volumes and the transient nature of the data.

The grooming strategy for a specific data type should take into account how fast the usefulness of the data decreases from time of collection and also how much data is collected on average over a time period. For example, the data in the alert_incoming table has a short shelf life. Real-time alerts are intended to address critical problems that can be resolved by taking action within a short timeframe, such as crashes of mission-critical applications or disruptive network failures. Because of these characteristics and because historical alert data is retained, real-time alert data is groomed aggressively.

It is important to ensure that the grooming schedule is taken into account if data is being warehoused or reports are being archived. If data is transferred less frequently than the grooming schedule for a type of data, data loss can occur. Similarly, report archiving schedules must take into account the grooming schedule to avoid introducing gaps in

historical reports.

You can monitor the status of grooming jobs by displaying the grooming log (**Server Status > Grooming Log**). The log displays the following information:

- **Data Area**—The type of data on which grooming was performed.
- **Grooming Job Name**—The name of the grooming job run, such as `core_groom_instance`.
- **Job Status**—The completion status of the job, such as “The maintenance job succeeded.”
- **Start Time**—The date and time that the grooming job started.
- **Duration**—The elapsed time taken by the grooming job. Note that in the case of smaller databases, grooming jobs may show a duration of zero time.

Managing Maintenance Jobs

In addition to grooming, there are a number of other maintenance jobs which are performed by an EdgeSight Server. These include dealing with data uploads and clearing caches and temporary storage areas. Each job is associated with a schedule, either Fifteen Minute or Nightly. The Fifteen Minute schedule runs jobs at fifteen minute intervals whenever EdgeSight Server is operational and is not configurable. The Nightly schedule runs jobs once a night and can have a start time configured. By default, the start time is five minutes after midnight based on server time. This allows the job to run to completion when the fewest users are active. The following table shows which console pages to display when managing maintenance jobs.

Console Page	Operations
Server Configuration > Data Maintenance > Jobs	Display job schedules, edit the start time for the Nightly schedule, and manually run jobs associated with schedules.
Server Status > Job Status	Determine when jobs last ran and their completion status. You can also display the overall duration of the set of jobs and the last run duration of individual jobs.
Server Status > Job Log	Display the run history of individual jobs, including result, duration, and start time.

Handling Unmanaged Devices

Unmanaged devices are systems running an EdgeSight agent that are not associated with a company and department. The agent can communicate with the server and be included in the list of unmanaged devices as long as it has a valid server and port specified during installation. Devices may be unmanaged due to the following reasons:

- The Company information provided by the agent when it registered with the server did not match an existing company.
- The Automatically register agents setting is disabled. (For more information, see “Agent Registration Settings” in [Managing Company Properties](#).)
- A database corruption has occurred on the device and recovery has failed.

You can monitor the number of unmanaged devices from the System Status page or by navigating to **Server Settings > Configuration > Unmanaged Devices**. The Unmanaged Devices page allows you to move a device to a company and department. Devices running EdgeSight for XenApp 5.0 agents can only be moved to the PS Farms department. All other devices can be moved to the Endpoints department. For agents that were previously registered with the server, the department to which the device last uploaded data is displayed in the **Registered Org** field.

The EdgeSight Agent on an unmanaged device collects data and uploads data to the server but will not appear in any historical or real-time reports. The data is subject to grooming, so allowing devices to remain unmanaged for lengths of time may result in lost data. Review the **Last Upload** field to determine when the agent on the device last communicated with the server.

Displaying Agent Database Broker Status

The configuration pages under the Agent Database Broker folder (Pools, Agent Database Servers, and Broker History) only display data if the EdgeSight Server is acting as a database broker for EdgeSight for Endpoints Agents installed on virtual desktops in a pooled environment. Although the database broker components are included in all EdgeSight Server installations, they are not used unless the server is specified as the database broker during the Agent Database Server and the EdgeSight Agent installations. For a description of the various components required for monitoring virtual desktops, see [Installing EdgeSight for Monitoring Virtual Desktops](#).

These pages reflect the status reported by Agent Database Servers, pools, and devices (in this case, virtual desktops running EdgeSight agents). In most cases, actions taken on these pages are housekeeping changes, such as deleting an unused pool or deleting stranded registration information for an Agent Database Server. Actions which directly affect your environment are rebalancing pools and enabling/disabling Agent Database Servers.

Displaying Pool Status and Rebalancing Pools

Use the Pools page (**Configuration > Server Configuration > Agent Database Broker > Pools**) to display information about pools (named groups of virtual desktops). The pool name corresponds to the XenDesktop desktop group name. In addition to displaying pool status, you can rebalance or delete pools.

The rebalance feature allows you to manually force a redistribution of agents in relation to database servers. The agents are not immediately rebalanced; the redistribution takes place over time as virtual desktops are shut down and rebooted.

Caution: Rebalancing agents in a pool across the database servers results in the loss of EdgeSight Agent data stored on those servers. Do not perform a manual rebalancing if you need to preserve agent data.

Deleting pools is a housekeeping function that should be performed when all the agent database servers associated with a pool have been deleted. For more information about pool rebalancing and deletion, see the “Pools” topic in online help.

Displaying Database Server Status

Use the Agent Database Servers page (**Configuration > Server Configuration > Agent Database Broker > Agent Database Servers**) to display current server status and to perform actions related to all the agent database servers which have registered with the database broker components of EdgeSight Server. You can disable/enable and delete servers.

If maintenance is required or a problem has occurred on a database server, you can disable the database server. Disabling a server means that the database broker components of EdgeSight Server do not broker the server to new agents. The agents already using the database server continue to store data in the database. Once the maintenance has been performed or the issue resolved, you can enable the server to make it available for

brokering to agents.

Deleting an agent database server only deletes the registration data stored on the EdgeSight Server database, such as the agent database server name, port, and pool association. The feature is designed to allow you to remove a stranded registration for a server which has been uninstalled or assigned to another EdgeSight Server.

For more information on server status, disabling/enabling servers, and deleting servers, see the “Agent Database Servers” topic in online help.

Displaying Broker History

Use the Broker History page (**Configuration > Server Configuration > Agent Database Broker > Broker History**) to display status messages for EdgeSight Agent Database Servers, pools, and devices. The message list can be filtered by server, pool, or device, providing a chronological history of the selected component. Most messages are informational, but errors are displayed for agents which are unable to connect to a database server. Note that long error strings are truncated to about 512 characters. See the “Broker History” online help topic for more information on individual columns in the Broker History table.

Troubleshooting Database Broker Issues

You can enable detailed logging for use in debugging broker issues on the **Agent Database Broker** tab at **Server Configuration > Settings**, as described in “Agent Database Broker Logging” in [Configuring Server Settings](#).

During installation, an agent can be configured to contact the EdgeSight Server acting as a database broker to receive a database connection string. If the fails to get a database connection, the agent shuts down and writes error information to the local SYS_EVENT_TXT.TXT log. If the File Monitor service on the agent is functioning properly, a copy of this file will be copied to the agent data file share. If the problem is that an incorrect path was supplied for the database broker, you can change configuration settings using the Citrix System Monitoring Agent control panel applet. However, you must make those changes on the base image in order for them to be propagated to all desktops. For more information on installing and configuring agents in a pooled environment, see [Installing EdgeSight for Monitoring Virtual Desktops](#).

Displaying and Responding to Server Messages

The Messages page (**Server Status > Messages**) displays status and event messages for EdgeSight Server and for devices running EdgeSight Agents. You can filter the list of messages by message type (All Types, Error, Warning, Informational, New Device, or Active Monitoring) and by company (All Companies, No Company Specified, or a specific company).

Managing Server Scripts

The Server Script Host page (**Server Status > Server Script Host**) displays the status of services on EdgeSight Server. These services include basic server functions, such as alert, payload and crash file handling, and maintenance functions, such as the cleanup of temp folders and crash report folders. Each service has an associated log file which may be helpful in isolating problems with server operations. You can also start and stop services, although this should generally be done at the direction of Citrix Technical Support.

EdgeSight Feature Availability

The data collected and displayed depends on the type and version of EdgeSight Agent installed and the version of the XenApp server or Presentation Server being monitored. Feature availability information can be broken down as follows:

- by agent type
- by agent version
- by XenApp or Presentation Server version

EdgeSight Feature Availability By Agent Type

This section provides information about what features will be displayed and data collected based on the Agent Support settings (**Configure tab > Server Configuration > Settings**). The server features are broken out by the tab on which they appear in the EdgeSight Server Console or by feature type, such as alerts. An X indicates that the feature or data is present. If the column is blank, the feature or data is not present.

Note: The agent support settings only control the display of data on the console; they do not affect the collection of data by agents.

EdgeSight provides the following types of agents:

- **EdgeSight for Endpoints** – Endpoint agents provide monitoring and data collection for endpoint devices.
- **EdgeSight for Virtual Desktops Agent** – Virtual desktop agents monitor instances of XenDesktop. In addition to monitoring system, application, and network performance, it collects ICA channel data including XenDesktop multi-media counters, collects end user experience metrics, and alerts on XenDesktop session performance. Note that this agent does not provide monitoring of the Desktop Delivery Controller (DDC).
- **EdgeSight for XenApp, Basic** – Basic agents require only that you have a XenApp Enterprise license available on your Citrix License Server.
- **EdgeSight for XenApp, Advanced** – Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix License Server.

Monitor Tab

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Alert Console	X	X	X	X
Dashboard	X	X	X	X
Alert List	X	X	X	X
Farm Monitor		X	X	X

Troubleshoot Tab

The following features are available on the **Troubleshoot** menu:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Device Troubleshooter	X	X	X	X
Device Process List	X	X	X	X
Find EdgeSight Servers	X	X	X	X
Device Trace Route	X		X	X
User Troubleshooter		X	X	

The following features are available on the **Real-time Reports** menu:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Device Summary	X	X	X	X
Alert List	X	X	X	X
System Performance	X	X	X	X
System Compare	X	X	X	X
Custom Performance Counters	X	X	X	X
Network Performance	X		X	X
XenApp Summary		X	X	
XenApp User Summary			X	

Plan and Manage Tab

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Overview	X	X	X	X
Device Summary	X	X	X	X
Process Performance Summary by Process	X	X	X	X
Process Summary	X	X	X	X
Network Summary	X		X	X
Network Summary by Site	X		X	X

EdgeSight Feature Availability By Agent Type

Network Transaction Summary	X		X	X
Process Stability Summary by Process	X		X	X
XenApp Summary		X	X	
User Summary for a User Group			X	X
XenApp User Summary			X	
XenDesktop Summary				X
XenDesktop User Summary				X

Track Usage Tab

Note: Citrix Licensing reports are not dependent on EdgeSight Agents and are therefore not affected by agent support settings.

The following **Published Applications** features are available:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Launch Summary for a Farm			X	
Launch Summary for a User Group			X	
Summary for a Farm			X	
Summary for a User Group			X	
Users Summary for a Farm			X	
Users Summary for a User Group			X	

The following **Session Duration** features are available:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Session Duration for a Farm		X	X	X
Session Duration for a User Group		X	X	X

Browse Tab

Note: The License Server Monitor Archive report is not dependent on EdgeSight Agents and is therefore not affected by agent support settings.

The following reports will display data for all agent support settings (Endpoint, XenApp Basic, XenApp Advanced, and Virtual Desktop):

- Alerts
- Asset Changes
- Assets for a Device
- Device Archive
- Device Summary
- Error Archive
- Event Log Alerts
- Event Log Alerts for a User Group
- New Processes
- Process CPU
- Process Cumulative CPU
- Process Memory Usage
- Process Pages Per Second
- Process Performance Archive
- Process Performance Summary by Process
- Process Stability Summary by Process
- Process Summary
- Process Thread Count
- Process Usage
- Process Usage Archive
- Real-time Alert List
- Real-time Device Summary
- Real-time System Compare
- Real-time System Performance
- Software Asset Changes
- System CPU
- System CPU Summary
- System Disk Usage

- System Disk Usage Archive
- System Disk Usage Summary
- System Kernel for a Device
- System Memory Summary
- System Memory Usage
- System Page Faults
- System Performance Archive
- Trace Event Archive

The following reports will display data for the Endpoint, XenApp Basic, and XenApp Advanced agent support settings, but not for the Virtual Desktop support setting:

- Real-time XenApp Summary
- Reboots

The following reports will display data for the Endpoint, XenApp Advanced, and Virtual Desktop agent support settings, but not for the XenApp Basic support setting:

- Hardware Alerts
- Hardware Asset Changes
- Network Connection Archive
- Network Summary
- Network Summary by Site
- Network Transaction Archive
- Network Transaction Summary
- New Sites
- Port Network Delay
- Port Network Round Trip Time
- Port Network Volume
- Port Web Errors
- Process Errors
- Process Errors for a User Group

- Process Faults
- Process Faults for a User Group
- Process Network Delay
- Process Network Volume
- Process Not Responding Alerts
- Process Not Responding Alerts for a User Group
- Real-time Network Performance
- Site Network Delay
- Site Network Errors
- Site Network Round Trip Time
- Site Network Volume
- Transaction Network Delay
- Transaction Network Round Trip Time
- Transaction Network Volume
- Transaction Web Errors
- Visited Sites

The following reports will display data for the XenApp Basic, XenApp Advanced, and Virtual Desktop agent support settings but not for the Endpoint support setting:

- Environmental Usage
- Environmental Usage Archive
- Session Client Type
- Session Duration
- Session Duration for a User Group
- System Memory for a User Group
- User Logon Details
- User Logon Details for a User Group

The Real-time XenApp User Summary report will display data for the Endpoint and XenApp Advanced agent support settings but not for the XenApp Basic and Virtual Desktop agent support settings.

The following reports will display data for the XenApp Basic and XenApp Advanced agent support settings but not for the Endpoint and Virtual Desktop agent support settings:

- Session Counts
- CPU Utilization Management
- IMA Service Availability
- IMA Service State
- Session Login Time
- Session Login Time for a User Group
- XenApp Server Utilization
- XenApp Summary
- XenApp System Performance Archive

The following reports will display data for the XenApp Advanced and Virtual Desktop agent support settings but not for the XenApp Basic and Endpoint agent support settings:

- Session Auto-Reconnects
- Session Client and Server Startup Duration
- Session Client Startup Duration
- Session Client Startup Time Archive
- Session Memory
- Session Network Bandwidth Used
- Session Network Delay
- Session CPU
- Session CPU for a User Group
- Session Network Delay for a User Group
- Session Network Round Trip Time
- Session Network Round Trip Time for a User Group
- Session Network Volume
- Session Network Volume for a User Group
- Session Page Faults

- Session Performance Archive
- Session Server Startup Duration
- Session Server Startup Time Archive
- Session Startup Duration Details
- Site Network Errors for a User Group
- User Logon Counts
- User Summary for a User Group
- ICA Audio I/O
- ICA Client Version
- ICA Drive I/O
- ICA Printer I/O
- ICA Session Compression
- ICA Session I/O
- ICA Session Round Trip Time
- ICA Session Round Trip Time Archive
- ICA Session Round Trip Time for a User Group
- ICA Session Traffic
- ICA Session Traffic for a User Group
- ICA Video I/O

The following reports will display data only for the XenApp Advanced agent support setting but not for the Endpoint, XenApp Basic and Virtual Desktop agent support settings:

- Published Application Launch Archive
- Published Application Launch Count - Details
- Published Application Launch Count for a User Group - Details
- Published Application Launch Summary
- Published Application Launch Summary for a User Group
- Published Application Summary
- Published Application Summary for a User Group

- Published Application User Count - Details
- Published Application User Count for a User Group - Details
- Published Application User Summary
- Published Application User Summary for a User Group
- XenApp User Summary
- Application Response Failures
- Application Response Time
- Application Response Time for a Test
- ICA Session Latency
- ICA Session Latency for a User Group

The following reports will display data only for the Virtual Desktop agent support setting but not for the Endpoint, XenApp Basic and XenApp Advanced agent support settings:

- HDX MediaStream I/O
- HDX Plug-n-Play I/O
- XenDesktop Summary
- XenDesktop User Summary

Alerts

The following alerts are generated for all agent support settings (Endpoint, XenApp Basic, XenApp Advanced, and Virtual Desktop):

- Application Performance
- High Application Resource Usage
- New Process
- System Disk Bottleneck
- System Low Resources
- System Performance
- System Slowdown
- System Thrashing

- Thrashing Application
- Windows Event Log
- Windows Event Log: Application Error
- Windows Event Log: Security Audit Failure
- Windows Event Log: System Error

The Device Reboot alert is generated for the Endpoint, XenApp Basic, and XenApp Advanced agent support settings but not for the Virtual Desktop support setting.

The following alerts are generated for the Endpoint, XenApp Advanced, and Virtual Desktop agent support settings but not for the XenApp Basic support setting:

- Application Error
- Light Trace Event
- Network Connection Performance Exceeded SLA
- Network Socket Error
- Network Transaction Failure
- Network Transaction Performance Exceeded SLA
- Plug and Play Hardware Change
- Process Fault
- Process Hung
- Process Snapshot

The following alerts are generated for the XenApp Basic, XenApp Advanced, and Virtual Desktop agent support settings but not for the Endpoint support setting:

- Print Services Failure
- Session Performance
- Slow ICA Connection

The Physical Disk Failure alert is generated for the Endpoint and XenApp Advanced agent support settings but not for the XenApp Basic and Virtual Desktop support settings.

The following alerts are generated for the XenApp Basic and XenApp Advanced agent support settings but not for the Endpoint and Virtual Desktop agent support settings:

- Active Session Count High

- Client Update Communication Failure
- Client Update Database File Read Failure
- Client Update Database Read Failure
- Client Update Directory Read Failure
- Client Update File Cache Failure
- Client Update File Enumeration Failure
- Client Update ICA File Read Failure
- Client Update Installation Commencement Failure
- Client Update Installation Configuration Read Failure
- Client Update Insufficient Disk Space
- Client Update Insufficient Permissions Error
- Client Update Memory Allocation Failure
- Client Update New Version Send Failure
- Client Update Termination Failure
- Client Update Upgrade Failure
- Configuration Logging Database Unavailable
- Dominant Session
- Excess Disconnected Sessions
- Farm Data Store Connection Failure
- Health Monitoring and Recovery Action Failure
- Health Monitoring and Recovery Test Failure
- IMA Service is Unresponsive
- License Server Connection Failure
- Maximum Farm Connections Exceeded
- Number of Servers in a Zone is Too High
- Published Application Concurrent Usage Limit
- Session Idle too Long
- Session in Down State

- Terminal Server Client Connection Error
- Terminal Server License Server Discovery Failure
- Thrashing Session
- XenApp System Performance
- Zone Data Collector Election Triggered
- Zone Elections too Frequent

The following alerts are generated for the XenApp Advanced agent support setting but not for the Endpoint, XenApp Basic and Virtual Desktop agent support settings:

- Application Response Failure
- Application Response Time
- Session Disconnected
- Session Performance (without EUEM)
- Slow ICA Connection (without EUEM)

The following alerts are generated only for the Virtual Desktop agent support setting but not for the Endpoint, XenApp Basic and XenApp Advanced agent support settings:

- Desktop Registration Failed
- Heartbeat Halted
- VDA Failed to Start

Agent Data Collection

Data Type	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Custom Performance Monitoring	X	X	X	X
Device Asset Changes	X	X	X	X
Disk Usage	X	X	X	X
Light Trace Events	X	X	X	X
Process Performance	X	X	X	X
Process Usage	X	X	X	X
Remote Agent Access	X	X	X	X

System Performance	X	X	X	X
Application Errors	X		X	X
Application Not Responding	X		X	X
Network Performance	X		X	X
Network Transactions	X		X	X
Process Crashes/Snapshots	X		X	X
System Performance		X	X	X
IMA Service State		X	X	
EUEM Data			X	X
ICA Channel Performance			X	X
Print Services			X	X
Session Performance			X	X
Active Application Monitoring			X	

Configure Tab

All Configure tab features are displayed to users with administrative privileges with the following exceptions based on agent support setting:

- If EdgeSight for XenApp support is disabled, the Farm Authentication page is not displayed.
- If EdgeSight for XenApp support is disabled or set to Basic, the IP Ranges page and the EdgeSight Licensing page are not displayed.
- If only EdgeSight for Virtual Desktop agent support is enabled, the EdgeSight Licensing page is not displayed.

Active Application Monitoring Support

The EdgeSight for XenApp Agent running in Advanced Mode is required for the recording of Active Application Monitoring scripts.

EdgeSight Feature Availability By Agent Version

The type of data collected depends on the version of EdgeSight Agent installed on a device. Some reports and SQL views will not return data if the collection of that type of data is not supported by the agent.

EdgeSight for Virtual Desktop Agent and EdgeSight for XenApp 5 Agent

The EdgeSight for Virtual Desktops Agent is required for collecting the data displayed in the following reports:

- XenDesktop Summary
- XenDesktop User Summary
- HDX MediaStream I/O
- HDX Plug-n-Play I/O

Either the EdgeSight for XenApp agent (for 5.x versions of XenApp) or the EdgeSight for Virtual Desktops agent is required for the collection of data displayed in the following new reports:

- ICA Client Version
- User Logon Counts

See the Virtual Desktop SQL Views topic in the online help for definitions of the various SQL views.

Note: Many of the views are shared by the XenApp and XenDesktop monitoring capabilities of EdgeSight:

- Views named vw_vda_* are only for use in retrieving data from virtual desktops.
- Views named vw_xa_vda_* can be used to retrieve data from either a XenApp server or a virtual desktop.

Select the view that matches the types of machines in your environment. Note that EdgeSight does not currently monitor Desktop Delivery Controller (DDC) systems.

EdgeSight for XenApp 6 Agent

EdgeSight for XenApp 6 Agent 5.3 (64-bit) was designed to monitor XenApp 6.0 systems; it does not monitor earlier XenApp versions. EdgeSight Server 5.3 included a new SQL view for published application events (vw_ctx_archive_published_app_event). Published application event data was collected by both the EdgeSight 5.2 agents and EdgeSight for XenApp 6 Agent 5.3.

For the EdgeSight 5.4 release, this agent was replaced by the Edgesight for XenApp 6 Agent 5.4, which can monitor XenApp 6.0 and XenApp 6.5 systems. There are no changes to agent data collection.

Data Collection by Presentation Server or XenApp Server Version

The type of data collected and displayed depends on the version of Presentation Server or XenApp Server being monitored, as well as on the version of EdgeSight Agent installed on a device. Reports and SQL views can return data only if the collection of that type of data is supported by the version of the server being monitored and also by the version of the agent.

Reports

Reports display data based on the version of XenApp or Presentation Server with an EdgeSight agent; in some cases, the display of data may be limited by the use of older agent versions. For information on the relationship of agent version to data collection, see [EdgeSight Feature Availability By Agent Version](#).

Note: The License Server Monitor Archive report contains data collected by the EdgeSight Server from a Citrix License Server. See the System Requirements topic for your EdgeSight release for more information.

The XenDesktop Summary and XenDesktop User Summary reports contain data on XenDesktop.

The following reports display data for all supported versions of XenApp or Presentation Server:

- Alerts
- Asset Changes
- Assets for a Device
- CPU Utilization Management
- Device Archive
- Device Summary
- Environmental Usage
- Environmental Usage Archive
- Error Archive
- Event Log Alerts
- Event Log Alerts for a User Group

- Hardware Alerts
- Hardware Asset Changes
- ICA Audio I/O
- ICA Client Version
- ICA Drive I/O
- ICA Printer I/O
- ICA Session Compression
- ICA Session I/O
- ICA Session Round Trip Time
- ICA Session Round Trip Time Archive
- ICA Session Traffic
- ICA Session Traffic for a User Group
- ICA Video I/O
- IMA Service Availability
- IMA Service State
- Network Connection Archive
- Network Summary
- Network Summary by Site
- Network Transaction Archive
- Network Transaction Summary
- New Processes
- New Sites
- Port Network Delay
- Port Network Round Trip Time
- Port Network Volume
- Port Web Errors
- Process CPU
- Process Cumulative CPU

- Process Errors
- Process Errors for a User Group
- Process Faults
- Process Faults for a User Group
- Process Memory Usage
- Process Network Delay
- Process Network Volume
- Process Not Responding Alerts
- Process Not Responding Alerts for a User Group
- Process Pages Per Second
- Process Performance Archive
- Process Performance Summary by Process
- Process Stability Summary by Process
- Process Summary
- Process Thread Count
- Process Usage
- Process Usage Archive
- Published Application Launch Archive
- Published Application Launch Count - Details
- Published Application Launch Count for a User Group - Details
- Published Application Launch Summary
- Published Application Launch Summary for a User Group
- Published Application Summary
- Published Application Summary for a User Group
- Published Application User Count - Details
- Published Application User Count for a User Group - Details
- Published Application User Summary
- Published Application User Summary for a User Group

- Real-time Alert List
- Real-time Device Summary
- Real-time Network Performance
- Real-time System Compare
- Real-time System Performance
- Real-time XenApp Summary
- Real-time XenApp User Summary
- Reboots
- Session Auto-Reconnects
- Session Client and Server Startup Duration
- Session Client Startup Duration
- Session Client Startup Time Archive
- Session Client Type
- Session Counts
- Session CPU
- Session CPU for a User Group
- Session Memory
- Session Network Bandwidth Used
- Session Network Delay
- Session Network Delay for a User Group
- Session Network Round Trip Time
- Session Network Round Trip Time for a User Group
- Session Network Volume
- Session Network Volume for a User Group
- Session Page Faults
- Session Performance Archive
- Session Server Startup Duration
- Session Startup Duration Details

- Site Network Delay
- Site Network Errors
- Site Network Errors for a User Group
- Site Network Round Trip Time
- Site Network Volume
- Software Asset Changes
- System CPU
- System CPU Summary
- System Disk Usage
- System Disk Usage Archive
- System Disk Usage Summary
- System Kernel for a Device
- System Memory for a User Group
- System Memory Summary
- System Memory Usage
- System Page Faults
- System Performance Archive
- Trace Event Archive
- Transaction Network Delay
- Transaction Network Round Trip Time
- Transaction Network Volume
- Transaction Web Errors
- User Logon Counts
- User Logon Details
- User Logon Details for a User Group
- User Summary for a User Group
- Visited Sites
- XenApp Summary

- XenApp System Performance Archive
- XenApp User Summary

The following reports display data for supported versions of XenApp, but not for Presentation Server:

- Application Response Failures
- Application Response Time
- Application Response Time for a Test
- HDX MediaStream I/O
- HDX Plug-n-Play I/O
- Session Duration
- Session Duration for a User Group
- XenApp Server Utilization

Agent Data Collection

The following types of data are collected by an agent in Advanced Mode, for all supported versions of XenApp or Presentation Server:

- Application Errors
- Application Not Responding
- Session Performance
- System Performance
- Custom Performance Monitoring
- Device Asset Changes
- Disk Usage
- Light Trace Events
- Network Performance
- Network Transactions
- Process Crashes/Snapshots
- Process Performance
- Process Usage

- Remote Agent Access
- System Performance
- EUEM Data
- ICA Channel Performance
- IMA Service State
- Print Services*

Note: * Due to high performance costs, printer tracking is disabled by default when you install the agent. This means that ICA Printer I/O report will not contain printer name or printer driver information. To enable printer tracking, set the following registry setting to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\System  
Monitoring\Agent\Ctrx\4.00\DisablePrinterTracking
```

Once printer tracking is enabled, this setting will be preserved during upgrades of the EdgeSight for XenApp agent.

The following data is collected by an agent in Advanced Mode for all supported versions of XenApp, but not for Presentation Server:

- Active Application Monitoring (AAM)

Integrating EdgeSight Alerts with Microsoft System Center Operations Manager

You can deploy and configure software to forward EdgeSight alerts to Microsoft® System Center Operations Manager 2007 (SCOM) and to monitor the health of EdgeSight Servers. The required software includes the Citrix EdgeSight Management Pack and EdgeSight Server 5.2 or later. Currently, only alerts generated by EdgeSight for XenApp agents can be forwarded.

About the Citrix EdgeSight Management Pack

The Citrix EdgeSight Management Pack, along with the EdgeSight alert actions feature, facilitates alert forwarding from an EdgeSight Server to SCOM. The Management Pack also includes monitors, rules, views, and tasks for monitoring the health of Citrix EdgeSight Servers.

When you import the EdgeSight Management Pack, it discovers all EdgeSight Servers and implements rules that receive and display the alerts forwarded by the EdgeSight Server.

EdgeSight Management Pack includes the following features:

- Collects and displays alerts forwarded by EdgeSight Server
- Monitors the health of the Citrix RSSH Admin and Citrix RSSH Application Manager services
- Remotely restarts the Citrix RSSH Admin and Citrix RSSH Application Manager services if they are stopped
- Collects EdgeSight errors written to the Application Event Log on the EdgeSight Server
- Provides multiple methods to launch the EdgeSight Server Console from within the Operations Manager console

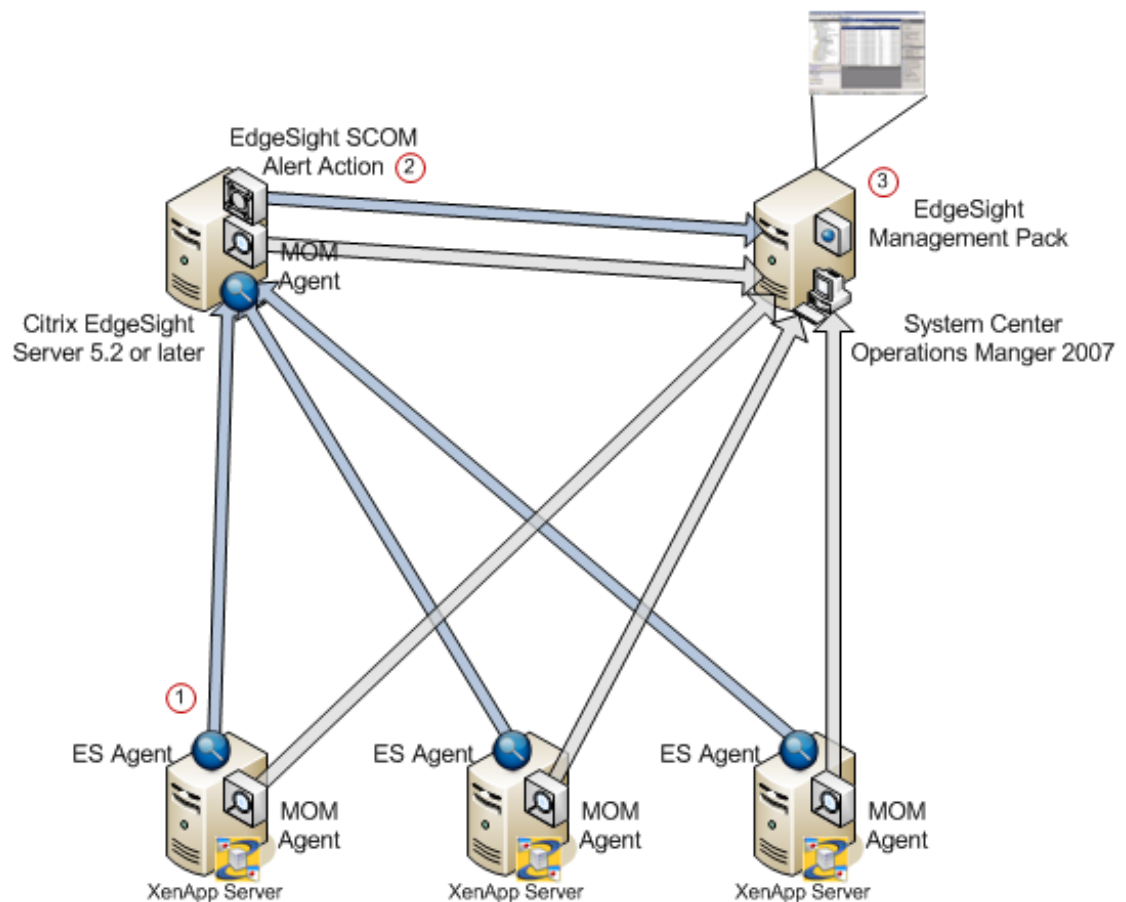
About the Forward to Microsoft System Center Operations Manager Alert Action

The EdgeSight alert actions feature is used to forward EdgeSight Alerts to the Operations Manager Root Management Server. The Forward to Microsoft System Center Operations Manager alert action allows you to specify an alert name, a root management server, and a set of credentials for authentication to that server.

Deployment Diagram

The following diagram illustrates communications between Citrix EdgeSight Server and SCOM. The EdgeSight Management Pack workflow is as follows:

1. The EdgeSight agent running on a XenApp server detects an error condition and sends an alert to the EdgeSight Server
2. An alert action on the EdgeSight Server forwards the alert to SCOM
3. The EdgeSight Management Pack, within SCOM, receives the EdgeSight alert and displays it in the Operations Manager Console; aggregating EdgeSight alerts with SCOM alerts into one logical view



System Requirements for EdgeSight Alert Integration with System Center Operations Manager

Citrix EdgeSight alert integration with System Center Operations Manager requires the Citrix EdgeSight MP file that you import into Operations Manager from the Operations Console.

Operations Manager 2007 Server

To use the Management Pack, you must be running Operations Manager 2007. The Operations Manager 2007 minimum hardware and software requirements can be found here: <http://www.microsoft.com/systemcenter/operationsmanager/en/us/system-requirements.aspx>.

You must import the Citrix XenApp Management Pack v5.0 into Operations Manager prior to importing the EdgeSight Management Pack. The XenApp Management Pack is available on the XenApp Server Enterprise and Platinum Edition DVD or by download at www.citrix.com.

It is important to import the XenApp Management Pack files into Operations Manager in the following order:

1. Citrix.Library.mp
2. Citrix.PresentationServer.mp

The Citrix.LicenseServer.mp is also part of the XenApp Management Pack, but is not required by the EdgeSight Management Pack.

Note: Be sure to configure a Citrix Administrator Account “Run As Profile” with the Citrix administrator credentials after your import Citrix.PresentationServer.mp. Failure to complete this step can prevent Citrix servers from appearing in the Citrix Managed Servers group. See the *Management Pack for Operations Manager 2007 Administrator's Guide*, for XenApp 5.0 for Windows Server 2008 at <http://support.citrix.com/article/CTX116421> for detailed instructions.

XenApp 5 and Presentation Server 4.x Servers

You must install the Operations Manager Agent and the Citrix EdgeSight for XenApp Agent on all XenApp and / or Presentation Servers as described in *How to Deploy the Operations Manager 2007 Agent Using the Agent Setup Wizard* (<http://technet.microsoft.com/en-us/library/bb309515.aspx>).

Ensure the Citrix servers are properly discovered and monitored in both EdgeSight and Operations Manager.

EdgeSight Server

You must install the Operations Manager Agent on the EdgeSight Server to allow Operations Manager to discover and monitor the server, as well as receive alerts from the EdgeSight

Server. Installation procedures are provided in as described in *How to Deploy the Operations Manager 2007 Agent Using the Agent Setup Wizard* (<http://technet.microsoft.com/en-us/library/bb309515.aspx>).

You must also install the Operations Manager Console which includes libraries required for EdgeSight Server to communicate with the Operations Manager Root Management Server, as described in *How to Deploy an Operations Manager 2007 Operations Console Using the Setup Wizard* (<http://technet.microsoft.com/en-us/library/bb381292.aspx>).

Prerequisites Review

Note: These prerequisites are listed in the order in which they must be imported or installed.

Operations Manager 2007 Server

- Import Citrix.Library.mp
- Import Citrix.PresentationServer.mp

XenApp Servers

- Install EdgeSight Agent
- Install Operations Manager Agent

EdgeSight Server

- Install Operations Manager Agent
- Install Operations Manager Console or Operations Manager Authoring Console

Installing and Configuring Components

To integrate EdgeSight software with the System Center Operations Manager, you must complete the following tasks:

- Import the EdgeSight Management Pack
- Configure an alert action to forward alerts to SCOM
- Assign the alert action to an alert rule

Importing the EdgeSight Management Pack

1. Open the EdgeSight media, click on **Browse CD**, and go to `\installers\Management_Packs`.
2. Locate the file named `Citrix.EdgeSight.mp` and copy it to the default Management Pack folder (`%ProgramFiles%\System Center Management Packs\`) on any machine running the Operations Manager Console.
3. Log on to the Operations Manager server and open the Operations Console.
4. Select **Administration** in the view pane Select Management Packs from the Administration View.
5. Select **Import Management Pack(s)** from the Actions menu.
6. Browse to the `Citrix.EdgeSight.mp` Management Pack file and click **Open** to view the Import Management Packs dialog box.
7. Click **Import**.
8. After the Management Pack is successfully installed, Operations Manager automatically deploys it to all the managed computers in your management group. Please allow time for this process to complete.

Configuring the Alert Action

To configure Citrix EdgeSight Server to forward alerts to SCOM:

1. Launch the EdgeSight Server Console.
2. Click the **Configure** tab.
3. Under Company Configuration select **Alerts > Actions**.
4. Click the **New Alert Action** button.

5. Select the **Forward to Microsoft System Center Operations Manager** option and then click the **Next** button to start the Alert Actions Creation Wizard
6. If you want to use an existing configuration (root management server name and credentials), select one from the drop-down menu. Otherwise, proceed to the next step.
7. Enter the name or IP address of the Root Management Server for System Center Operations Manager. A fully qualified domain name (FQDN) is only required in those cases where it is needed to establish a connection between the EdgeSight Server and the Root Management Server.
8. Enter the credentials to be used when authenticating to the server.
9. Click the **Next** button once the Alert Action properties are set.
10. Review the Alert Action and then click **Finish** to save.

Once the alert action is created you must assign it to an alert rule.

Assigning the Alert Action to an Alert Rule

1. Click the **Configure** tab.
2. Under **Alerts > Rules.**, click on the edit icon of an existing alert rule to launch the Alert Rules Wizard.
3. Select **Change Alert Rule to Alert Action Mappings** and click the **Next** button.
4. On the Assign Alert Rule to a Department screen, select **All** or a specific department you want to assign this rule to, and click the **Next** button.
5. On the Assign Action to Alert Rule screen, pick **Select the Alert Actions** radio button, check the alert action you created in the previous section, and click the **Finish** button

Uninstalling the EdgeSight Management Pack

You can uninstall the Management Pack using the Operations Manager Console. Uninstalling the Management Pack removes all the references to it from the Operations Manager database, including the monitoring objects provided by the Management Pack along with any dynamically discovered event, performance, or alert data. For information about uninstalling management packs, see your Operations Manager documentation.

Using the Management Pack

This topic introduces you to the Citrix EdgeSight views, rules, monitors, and tasks that are included in the Management Pack. It explains how to configure the Management Pack for your site. The topics include:

- Citrix Managed Objects
- Citrix Views
- Starting the Citrix EdgeSight Management Console

About Citrix Managed Objects

The Citrix family of Management Packs monitors and reports on a number of Citrix-specific objects.

Object	Description
Citrix Deployment	Represents a discovered Citrix deployment that can consist of multiple farms, zones, and EdgeSight Servers
Citrix Managed Server	Represents a XenApp or Presentation Server monitored by Operations Manager. A managed server must be a server that is running a version of Presentation Server listed in “Citrix XenApp Server Managed Computers” (next) with an appropriate license. The server must also be running the Presentation Server Provider.
Citrix Unsupported Server	Represents a server not monitored by Operations Manager. An unsupported server is not running a version of Presentation Server listed in “Citrix XenApp Server Managed Computers” (next).
Citrix Unlicensed Server	Represents a server not monitored by Operations Manager. The server is running the Presentation Server Provider, but is unlicensed or missing a valid license. Note that Operations Manager checks the licenses on these servers hourly.
Citrix EdgeSight Server	Represents an EdgeSight Server monitor by Operations Manager. The server must be running EdgeSight for XenApp 5.0 or later with an appropriate license.
Citrix Server Application	An abstract class that represents a server running any Citrix server product. The Citrix Server Application class is the target for alerts forwarded by EdgeSight.

Citrix XenApp Server Managed Computers

In the Management Pack, a Citrix XenApp Server (displayed as Citrix Presentation Server) managed computer is a server that is running one of the following releases, with an appropriate license:

- Citrix Presentation Server 4.0, Enterprise Edition
- Citrix Presentation Server 4.5, Enterprise or Platinum Edition
- Citrix XenApp Server 5.0 or later, Enterprise or Platinum Edition

Servers running earlier versions of Presentation Server are considered unsupported computers, while servers that are not appropriately licensed are considered unlicensed computers. These computers are not monitored by the Management Pack, and will not appear in the deployment topology diagram.

Note: After licenses are allocated, computers running Presentation Server might not be recognized as managed until the next time Attribute Discovery runs. By default, this happens every 60 minutes.

About Citrix Views

The EdgeSight Management Pack inherits from, and integrates with, Citrix views available in the Citrix XenApp Management Pack. These views allow you to monitor events raised by both Operations Manager and EdgeSight for servers and server farms running Citrix XenApp and Presentation Server.

The Citrix EdgeSight Management Pack extends the Citrix Active Alerts view, All Citrix Events view, Citrix Deployment State view, and the Citrix Presentation Server Topology Diagram view. It also adds the Citrix EdgeSight folder which contains the Citrix EdgeSight Alerts view, the Citrix EdgeSight Console View, and the Citrix EdgeSight State view. The Citrix Performance view and Citrix Licensing view are not affected by the EdgeSight Management Pack.

Alert and Event Views

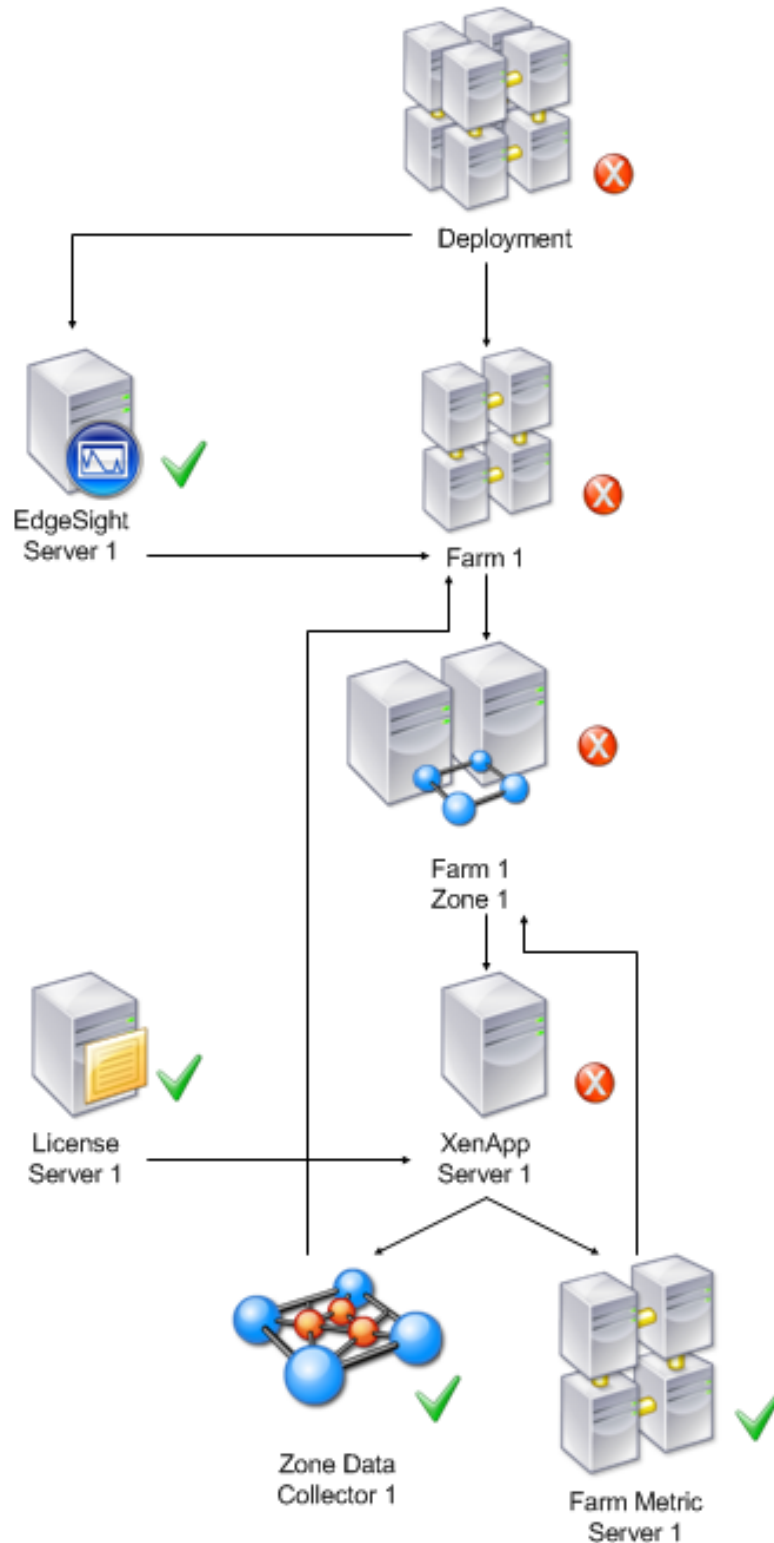
Alert and event views provide system administrators with real-time event and alert information. Alert views group alerts by severity, and event views sort events chronologically for ease of reference.

Alerts and events generated by the XenApp Management Pack rules and monitors and alerts forwarded by the EdgeSight Server are collected and displayed in these views. There are three Citrix alert and event views.

View	Description
All Citrix Events	Displays all the events raised by Citrix Presentation Server components and all events inserted by the EdgeSight alert actions on managed servers.
Active Alerts from Citrix Servers	Displays all unresolved alerts raised against managed servers by all management packs (not only the XenApp Management Pack).
Active Citrix Alerts	Displays all unresolved alerts raised by the XenApp Management Pack and by the EdgeSight Management Pack.

Citrix Server Topology Diagram View

The Citrix Server topology diagram view provides a hierarchical representation of a Citrix deployment, displaying farms, zones, license servers, XenApp Servers, and EdgeSight Servers and their relationships.



The topology view provides the following information:

- The name of the farm, zone, or server and the discovered properties of each object. The discovered properties of the EdgeSight Server object are:
 - EdgeSight Version Number
 - SQL Server Name
 - Database Name
 - Database Version
 - IP Address
 - EdgeSight admin console URL
 - Web Port
 - Last Update
- The current alert state, propagated up the tree so that state changes are visible even when the view is collapsed.

Citrix EdgeSight Folder

The EdgeSight Management Pack creates a new Citrix EdgeSight folder under the Citrix Presentation Server root folder. The Citrix EdgeSight folder contains an alert view, console view, and state view that contain information specific to the EdgeSight Server.

View	Description
Citrix EdgeSight Alerts	Displays all alerts raised by the alert action feature running on the EdgeSight Server.
Citrix EdgeSight Servers	Displays all the discovered Citrix EdgeSight Servers and their current health state.

Citrix EdgeSight Server Health Roll-up

Monitors represent the health state of a managed computer by evaluating rules against pre-defined criteria. The health state can be set to one of three conditions: Success, Warning, and Critical.

The EdgeSight Management Pack contains two Windows service monitors; one for the Citrix RSSH Admin Service and one for the Citrix RSSH Application Manager Service.

Monitor	Description
Citrix RSSH Aggregate	Health Roll-up Policy that displays the worst health state of the two RSSH Service monitors.

Citrix RSSH Admin Service	Monitors the state of the Citrix RSSH Admin Service. The health state is set to Critical when this service is stopped and Healthy when the service is running. The Monitor also includes a recovery task that will remotely restart the service and reset the monitor state when after recovery finishes.
Citrix RSSH Application Manager Service	Monitors the state of the Citrix RSSH Application Manager Service. The health state is set to Critical when this service is stopped and Healthy when the service is running. The Monitor also includes a recovery task that will remotely restart the service and reset the monitor state when after recovery finishes.

Starting the Citrix EdgeSight Console

To aid troubleshooting alerts forwarded to Operations Manager by EdgeSight Server, the EdgeSight Management Pack provides multiple ways to launch the EdgeSight Management Console from the Operations Manager console.

To start the EdgeSight Console:

1. Log on to the Operations Manager Console.
2. Navigate to the Monitoring View.
3. Perform one of the following:
 - In the Citrix Presentation Server Topology Diagram view, select an EdgeSight server icon, in the Detail View click on the EdgeSight Console URL property value or in the Actions pane, select **Start EdgeSight Management Console**.
 - In the Citrix EdgeSight Servers view, select an EdgeSight server, in the Detail View click on the EdgeSight Console URL property value or in the Actions pane, select **Start EdgeSight Management Console**.

Security Considerations

This topic provides information about Operations Manager actions accounts and using low-privilege accounts with the Citrix EdgeSight Management Pack and the SCOM alert action.

EdgeSight Management Pack

The EdgeSight Management Pack uses the default agent action account that is created when Operations Manager is first installed to perform discovery and run rules, tasks, and monitors. By default, Operations Manager assigns the Local System account as the agent action account. When running as Local System, the agent action account has all the privileges necessary to perform discovery and run rules, tasks, and monitors.

Low-Privilege Environments

You can use a low-privilege account for the agent action account; however the service recovery tasks require elevated rights. The low-privilege account must meet the following requirements:

- Member of the local users group
- Granted Log On Locally rights

With the low-privilege action account the following features are supported:

- EdgeSight Server Discovery
- EdgeSight RSSH service monitoring
- Launch the EdgeSight Console

With the low-privilege action account the following features are not supported:

- Recovery task to restart the Citrix RSSH Admin Service
- Recovery task to restart the Citrix RSSH Application Manager Service

EdgeSight Alert Action

The Alert Action includes credentials used for authentication. This account must be a member of the Operations Manager Administrators role to access the SDK Service. This account must also be a member of the administrator's Local Group on the EdgeSight Server so that the alert action can spawn a local process. The low-privilege section describes the minimum permissions required by this account.

Low-privilege Environments

The minimum privileges required by the SCOM administrator account are:

- Domain: Member of the Domain Users Global Group
- Operations Manager: Member of the Operations Manager Administrators role
- EdgeSight for XenApp 5.0 or later: Member of the Administrator Local Group on the EdgeSight Server

Troubleshooting EdgeSight

Troubleshooting License Server Monitoring

By setting the Polling Errors option on the License Servers page (**Configure > License Monitor Configuration > License Server**) to **Send Email**, you can ensure that email is sent to the EdgeSight Administrator if license server polling fails. The administrator has several options for gathering more information:

- Examine license server-related messages
- Examine the log file for the core_lsm_license_poller server script

In addition, license servers with polling errors are indicated by specific error or warning icons in the License Usage Summary and License Usage Trending reports available on the **Track Usage** tab. For more information on these reports, see the “License Usage Summary” and “License Usage Trending” topics in online help.

Note: The EdgeSight 5.4 License Server Monitoring feature only works with license servers that are running Citrix Licensing 11.9. Attempting to monitor an incompatible license server will generate an error during data polling.

License Server Monitoring Messages

You can display license server monitoring messages on the Messages page (**Server Status > Messages**). To isolate the messages, sort the messages by source and locate those with a source of License Server Monitor. Most of the messages relating to license server monitoring are informational and reflect actions taken on the EdgeSight Server, such as adding or deleting a license server configuration. These information messages include:

- New License Server Added
- License Server Deleted
- License Server was disabled
- License Server was re-enabled
- New Product Feature Code found on license server

The Polling Failed error message indicates that an attempt to poll a license server has failed, most likely due to the inability of the license server poller to connect to the license server. (In most cases, an error code of -96 is displayed.) The failure to connect could be due to the license server being down or a network problem.

License Server Poller Log File

You can display the license server poller log file on the Server Script Host page (**Server Status > Server Script Host**). Locate the core_lsm_license_poller script, right-click the menu button, and select **View Log**.

A normal polling sequence with no errors is similar to the following:

```
1/20/2010 8:12:36 PM: LicenseServerMonitor: OnTimer: begin
1/20/2010 8:12:36 PM: LicenseServerMonitor: PollLicenseServers: begin
1/20/2010 8:15:49 PM: LicenseServerMonitor: PollLicenseServers method invoked *****
1/20/2010 8:15:49 PM: LicenseServerMonitor: Begin polling Server LICSERVER01.mycompany.net on port 2700
1/20/2010 8:15:49 PM: LicenseServerMonitor: Total Polling Time: 0:0.93
1/20/2010 8:15:49 PM: LicenseServerMonitor: Polling Successful. Total Licenses Retrieved: 21
1/20/2010 8:15:49 PM: LicenseServerMonitor: Begin polling Server LICSERVER02.mycompany.net on port 2700
1/20/2010 8:15:49 PM: LicenseServerMonitor: Total Polling Time: 0:51.750
1/20/2010 8:15:49 PM: LicenseServerMonitor: Polling Successful. Total Licenses Retrieved: 300
1/20/2010 8:15:49 PM: LicenseServerMonitor: PollLicenseServers method completed. *****
```

An error in polling is logged as follows:

```
1/20/2010 9:26:31 PM: LicenseServerMonitor: Begin polling Server LICSERVER01.mycompany.net on port 2700
1/20/2010 9:26:31 PM: LicenseServerMonitor: Total Polling Time: 0:10.0
1/20/2010 9:09:18 PM: LicenseServerMonitor: Polling Failed. Error code: -96
1/20/2010 9:09:18 PM: LicenseServerMonitor: Error Message: 1/20/2010 9:07:06 PM: The License Server Mon
retrieve any license utilization data for server "LICSERVER01.mycompany.net", port 27000.
Contact your Citrix License Server Administrator.
```

Forward the log to your Citrix License Server Administrator for further investigation.

Troubleshooting Using Agent Log Files

There are several log files located on devices running the agent which can be used to help diagnose issues of agent to server communication. Note that for agents running on virtual desktops, the log files are copied to an agent data file share specified during agent installation.

- The system and application event logs (found in the event viewer)
- The main EdgeSight log file. The default location is:

```
%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\SYS_EVENT_TXT.txt
for Microsoft Vista and Windows 2008 systems
```

```
%ALLUSERSPROFILE%\Application Data\Citrix\System
Monitoring\Data\SYS_EVENT_TXT.txt for all other systems
```

- Individual worker log files. (See “Monitoring Workers” in [Configuring, Scheduling, and Running Workers](#) for more information on worker log files.) The default location is:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\EdgeSight\log` for Microsoft Vista and Windows 2008 systems

`%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data\EdgeSight\log` for all other systems

If you detect a problem that you cannot solve and need to contact Technical Support, please have the agent and server software version numbers at hand. To verify product version information:

- Agent: Open the SYS_EVENT_TXT file. When the agent starts up, it inserts a line similar to the following:

----- Starting Agent on machinename version 5.0.74.0 -----

- Server: Open the EdgeSight console and navigate to **Server Status > About**. The correct version is listed next to Reflectent.EdgeSight.Loader.dll.

EdgeSight 5.3

Citrix® EdgeSight™ is a performance and availability management solution for endpoint, XenDesktop, and XenApp systems. EdgeSight monitors applications, devices, sessions, license usage, and the network in real time, allowing users to quickly analyze, resolve, and proactively prevent problems.

In This Section

Under this node, you will find the following resources for EdgeSight:

About EdgeSight 5.3	An overview of EdgeSight and its features
Known Issues in EdgeSight 5.3	Known issues in this release
Fixed Issues in EdgeSight 5.3	Fixed issues in this release
System Requirements for EdgeSight 5.3	System requirements for this release
Install and Configure	Installation procedures for all EdgeSight components
Upgrading EdgeSight	Upgrade and uninstallation procedures
Managing EdgeSight	Component and configuration information
Integrating EdgeSight Alerts with Microsoft System Center Operations Manager	How to use EdgeSight with Microsoft System Center Operations Manager
Troubleshooting EdgeSight	Information on troubleshooting license server monitoring and agent log files

Can't find what you're looking for? If you're looking for documentation for previously released versions of this product, go to the Citrix Knowledge Center. For a complete list of links to all product documentation in the Knowledge Center, go to <http://support.citrix.com/productdocs/>

EdgeSight 5.3

Citrix® EdgeSight™ is a performance and availability management solution for endpoint, XenDesktop, and XenApp systems. EdgeSight monitors applications, devices, sessions, license usage, and the network in real time, allowing users to quickly analyze, resolve, and proactively prevent problems.

In This Section

Under this node, you will find the following resources for EdgeSight:

About EdgeSight 5.3	An overview of EdgeSight and its features
Known Issues in EdgeSight 5.3	Known issues in this release
Fixed Issues in EdgeSight 5.3	Fixed issues in this release
System Requirements for EdgeSight 5.3	System requirements for this release
Install and Configure	Installation procedures for all EdgeSight components
Upgrading EdgeSight	Upgrade and uninstallation procedures
Managing EdgeSight	Component and configuration information
Integrating EdgeSight Alerts with Microsoft System Center Operations Manager	How to use EdgeSight with Microsoft System Center Operations Manager
Troubleshooting EdgeSight	Information on troubleshooting license server monitoring and agent log files

Can't find what you're looking for? If you're looking for documentation for previously released versions of this product, go to the Citrix Knowledge Center. For a complete list of links to all product documentation in the Knowledge Center, go to <http://support.citrix.com/productdocs/>

About EdgeSight 5.3

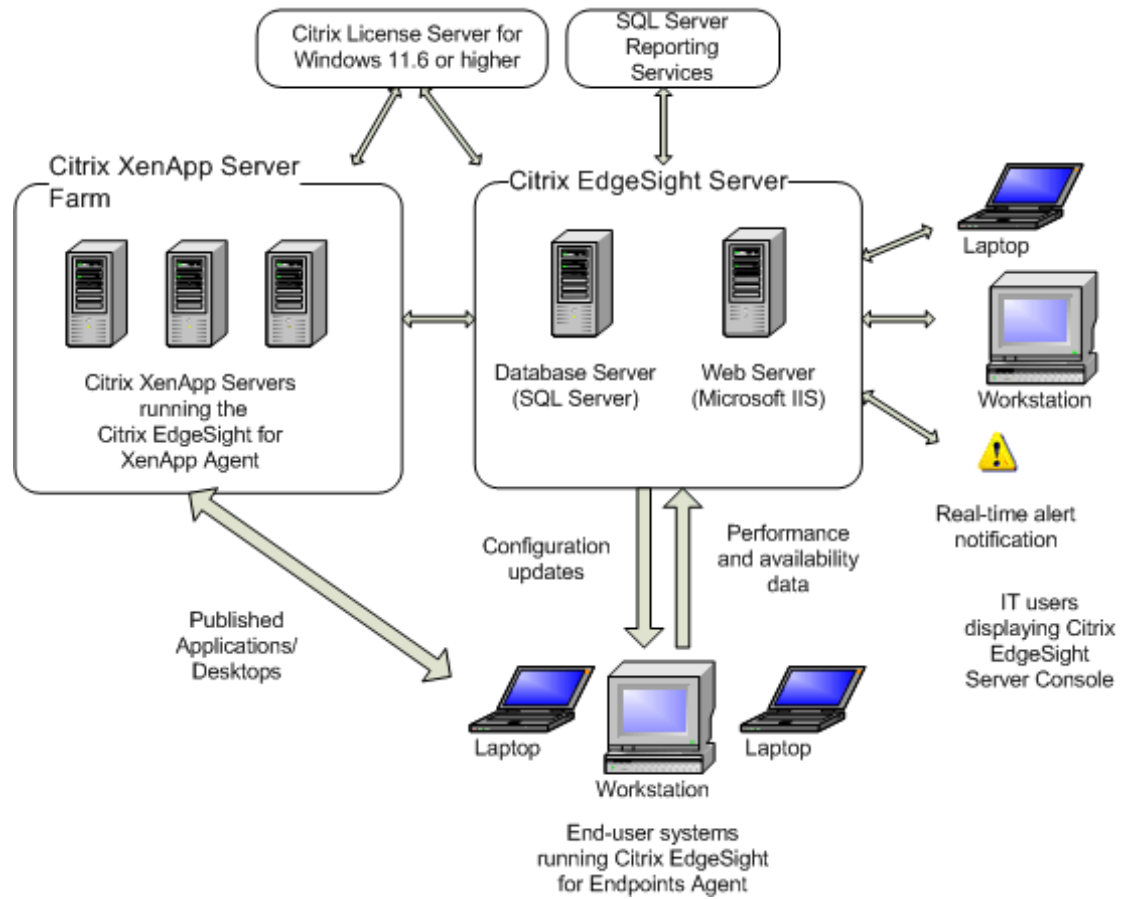
Citrix® EdgeSight™ is a performance and availability management solution for XenDesktop, XenApp and endpoint systems. EdgeSight monitors applications, devices, sessions, license usage, and the network in real time, allowing users to quickly analyze, resolve, and proactively prevent problems. You perform administrative tasks using the Citrix EdgeSight Server Console.

Citrix EdgeSight consists of the following components:

- EdgeSight Agents
- EdgeSight Server
- EdgeSight Server Console
- Citrix License Server

Additional components are required when monitoring virtual desktops, as described in “EdgeSight Components Required for Virtual Desktop Monitoring” in [EdgeSight Components](#). Note that EdgeSight requires the use of SQL Server Reporting Services for the generation of historical reports. See [System Requirements](#) for both agent and server system requirements.

The following figure shows the relationship between these components and the systems being monitored:



New Features for EdgeSight 5.3

This release of the product includes the following new features:

- Monitoring of Citrix License Servers and reporting on license usage by product group or individual products. The license servers to be monitored are specified at **Configure > License Monitor Configuration > License Servers**. License usage reports are available on the **Track Usage** tab.
- Monitoring of Published Applications and reporting on application launches and unique users. Published application reports are available on the **Track Usage** tab and the **Browse** tab.
- Monitoring of session duration by farm or user group. Session duration reports are available on the **Track Usage** tab and the **Browse** tab.
- EdgeSight Agent support for XenApp 6.
- EdgeSight for Endpoints Agent 5.3, EdgeSight for Virtual Desktops Agent 5.3, and EdgeSight for XenApp Agent 5.3. See "EdgeSight Agent Availability" later in this topic.
- In Active Application Monitoring, you can now configure the recorded bitmap size by navigating to **Options > Recorder Options** and entering the bitmap size. This enhancement addresses the previous limitation of a fixed 10x10 pixel recorded bitmap size. See "EdgeSight Active Application Monitoring Availability" later in this topic.
- Active Application Monitoring scripts can be run using a command line interface. For a description of the command line syntax, see the Controller Online Help or navigate to the folder containing the Controller EXE file and enter the following command:
`Controller.exe /?`. See "EdgeSight Active Application Monitoring Availability" later in this topic.

New reports and SQL views. See "New Reports and SQL Views" later in this topic.

Important: Note that EdgeSight Server 5.3 requires SQL Server 2005 or SQL Server 2008. If you are upgrading EdgeSight Server from a release prior to EdgeSight 5.2 using SQL Server 2000, you will also need to upgrade your SQL Server installation.

Note: If you are upgrading EdgeSight Server from a release prior to EdgeSight 5.2, note that support for the EdgeSight Virtual Desktop Agent is not enabled by default. To enable support after upgrading, open the EdgeSight Server Console and go to **Configure > Server Configuration > Settings** and set EdgeSight for XenDesktop Support to **On**.

EdgeSight Agent Availability

The initial release of the EdgeSight 5.3 media contained a new EdgeSight Agent, EdgeSight for XenApp 6 Agent x64 5.3 (64-bit), as well as the previous 5.2 SP1 releases of the EdgeSight for XenApp, EdgeSight for Endpoints, and EdgeSight for Virtual Desktops agents. Additional EdgeSight 5.3 agents are now available for download from the Citrix Downloads page at:

<http://www.citrix.com/English/ss/downloads/index.asp>

Important: EdgeSight 5.3 agents should be installed whenever possible because they include important fixes and enhancements. EdgeSight 5.2 SP1 agents should only be installed in the following cases:

- for use with an Edgesight Server which is still at version 5.2
- if other 5.2 SP1 agents are installed and you want to keep all agents at the same version for maintainability reasons

The following table lists the available EdgeSight Agents, which types of systems they are intended to monitor, and whether they reside on the media or are available for download:

Agent	Monitors...	Obtain from...
EdgeSight for XenApp 6 Agent x64 5.3 (64-bit)	XenApp 6.0	Media
EdgeSight for XenApp 5.3	XenApp 5.0 or 5.0 Feature Pack 2	Download
EdgeSight for Virtual Desktops 5.3	XenDesktop 4.0 or higher	Download
EdgeSight for Endpoints 5.3	Endpoints, XenDesktop 3.0	Download
EdgeSight for XenApp 5.2 SP1	XenApp 5.0 or 5.0 Feature Pack 2	Media
EdgeSight for Virtual Desktops 5.2 SP1	XenDesktop 4.0 or higher	Media
EdgeSight for Endpoints 5.2 SP1	Endpoints, XenDesktop 3.0	Media

EdgeSight Agents Supported for Upload to EdgeSight Server

Only the following agent types and versions are supported for upload to EdgeSight Server:

- EdgeSight for Endpoints 5.2 or higher
- EdgeSight for Virtual Desktops 5.2 or higher
- EdgeSight for XenApp 5.2 or higher

- EdgeSight for XenApp 6 Agent x64 5.3 (64-bit) running on 6.0 release of XenApp. This version of the agent is only supported for installation on XenApp 6.0 systems and cannot be used with previous XenApp versions.

EdgeSight Active Application Monitoring

EdgeSight Active Application Monitoring (AAM) 5.3 SP2 provides a number of security enhancements to the product. (For more information on these changes, see <http://support.citrix.com/article/CTX129699>.) No new end user features have been added for this release and no changes are required to tests or scripts. When upgrading from EdgeSight Active Application Monitoring 5.3 SP1, keep in mind the following:

- The user will be prompted to reset the security password during installation. This occurs when installing the Controller, the Launcher, or both components.
- Both the Controller and Launcher components must be upgraded.

If an old Controller is used with a new Launcher, the following error message is displayed in the Controller: One or more Launchers have reported an error and have exited. If a new Controller is used with a old Launcher, no error message is passed to the Controller. However, the error is logged in the trace/lservice.txt file located on the machine running the Launcher. For example: ControllerConnection. ControllerListen. Unrecognized message from Controller.

When establishing connections using ICA files, it is recommended that the ICA files be on the systems where the Launcher is running rather than on a remote file share.

A new AAM installation is now available for download from the Citrix Downloads page at:

<http://www.citrix.com/English/ss/downloads/index.asp>

New Reports and SQL Views

The following reports were added for this release:

- License Server Monitor Archive (XenApp)
- Published Application Launch Archive (XenApp)
- Published Application Launch Count - Details (XenApp)
- Published Application Launch Count for a User Group - Details (XenApp)
- Published Application Launch Summary (XenApp)
- Published Application Launch Summary for a User Group (XenApp)
- Published Application Summary (XenApp)

- Published Application Summary for a User Group (XenApp)
- Published Application User Count - Details (XenApp)
- Published Application User Count for a User Group - Details (XenApp)
- Published Application User Summary (XenApp)
- Published Application User Summary for a User Group (XenApp)
- Session Duration (XenApp and XenDesktop)
- Session Duration for a User Group (XenApp and XenDesktop)
- XenApp Server Utilization (XenApp)

Definitions of the following SQL views were added to the EdgeSight Server Console online help. To display definitions of these views, open online help and go to **SQL Views EdgeSight for XenApp SQL Views** and **SQL Views License Server Monitoring SQL View** respectively.

- vw_ctrx_archive_published_app_event - Citrix Published Application Events Archive
- vw_lsm_archive_license_statistics - License Server Monitor Archive

Known Issues in EdgeSight 5.3

The following is a list of known issues in this release. Read it carefully before installing the product.

Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent

There is a known incompatibility with the McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent.

Workaround: Do not install the agent on devices where this McAfee firewall is running. If McAfee HIPS is required on a computer running the EdgeSight Agent, please contact McAfee support for details on how HIPS can be configured to avoid this issue.

Installation Issues

Important: Before you install this product, make sure you consult [Install and Configure](#).

EdgeSight Agent Should Not Be Installed on Same Machine as the EdgeSight Server

The EdgeSight Agent should not be installed on the same machine hosting the EdgeSight Server. Problems with opening and saving payloads will occur on the server if the agent is subsequently uninstalled. Re-installing the server fixes this problem.

EdgeSight Agent Should Not Be Installed on Same Machine as the EdgeSight Agent Database Server

The EdgeSight Agent should not be installed on the same machine hosting the EdgeSight Agent Database Server due to registry issues. Uninstalling the agent and re-installing the server fixes this problem.

EdgeSight Server Installation Fails If Database Name Contains a Dot (.)

The EdgeSight Server install fails if there is a dot (.) in the database name. See [Installing EdgeSight Server](#) and Microsoft SQL Server documentation for information on valid database naming.

EdgeSight Server Should Be Installed Before the License Management Console in a Single Machine Installation

If the License Management Console and EdgeSight Server are installed on the same machine, install the EdgeSight Server before installing the License Management Console. Installing the License Management Console before installing the EdgeSight Server will result in the inability to access the EdgeSight Server web site.

Uninstalling EdgeSight Server on Windows Server 2008 When Using Non-Standard IIS Web Port

Attempting to uninstall EdgeSight Server on Windows Server 2008 through Add/Remove Programs when using a nonstandard IIS Web port (for example, port: 94) will fail.

Workaround: Run `setup.exe` and select **Remove**, or change the Web port to the default of 80, uninstall using Add/Remove Programs, then change the port back to the original setting.

Active Application Monitoring Issues

Secure Data Must Be Re-entered

Due to security enhancements, secure data such as user passwords are stripped from tests created in versions prior to Active Application Monitoring 5.3 SP1. All secure data needs to be re-entered prior to launching the test.

Japanese Character Display Issues

Japanese window title strings are not displayed correctly in Active Application Monitoring controller scripts when used together with XenApp 5.0 and XenApp Plugin 11.000. If you wish to use this configuration, please update the Plugin version to 11.100 or higher, by downloading Desktop Receiver - Version 11.100 or higher.

Recording or Editing Scripts to Replay Input of Japanese Characters Not Supported

Active Application Monitoring does not support recording or editing scripts to replay input of Japanese characters. This is a design limitation. For more information, please see <http://support.citrix.com/article/CTX119267>.

Desktop Not Properly Sized When Using ICA Client 11 and Windows 2008

When using the ICA version 11 client to connect to Windows 2008, the display of the desktop is not properly sized. This is a known ICA version 11 client issue and is currently being investigated.

Only ASCII ICA File Names are Supported

Only ICA files with ASCII names should be used for EdgeSight Active Application Monitoring connections. ICA files with non-ASCII character names may prevent users from recording and replaying scripts.

Only ASCII Launcher Names are Supported

Only ASCII Launcher names are supported. If you enter a non-ASCII Launcher name, the Could Not Connect to Launcher message box is displayed.

Fixed Issues in EdgeSight 5.3

Agent Fixes

This release of the product provides fixes for the following issues. The following fixes pertain to all EdgeSight 5.3 agents.

- Addressed an issue that prevented Java applications that allocate large amounts of memory from starting.
- Addressed an issue that caused Office 2010 applications running on 64-bit platforms to crash.
- Addressed an incompatibility that caused some applications to crash when the Symantec Protection Agent was installed.
- Addressed an issue that caused some Internet Explorer applications to crash when the agent was shutdown or restarted.

The following fixes only pertain to EdgeSight for XenApp agents.

- Addressed an incompatibility that caused some applications to crash when the XenApp Streaming Client was installed.
- Addressed a problem where when the agent could not collect EUEM metrics, it prematurely stopped trying to collect this data and sent an operational message to the EdgeSight Server.
- Addressed an issue that caused a payload error for duplicates in session auto-reconnect data.
- Addressed an issue where published applications without fully qualified pathnames were not detected.

Server Fixes

This release of the product provides fixes for the following issues:

- Enhanced the Farm Data Store Connection Failure alert to fire on additional events that indicated this condition.
- Addressed an issue that caused a payload error if a configuration check happened while a data payload was being uploaded.

System Requirements for EdgeSight 5.3

There are separate system requirements for EdgeSight Server and the various types of EdgeSight Agents, plus additional requirements depending on the environment being monitored.

Version Compatibility Matrices

Agents supported by EdgeSight Server 5.3 can monitor the following versions of XenApp:

Agent	XenApp 6.0	XenApp 5.5	XenApp 5.0	XenApp 4.5
EdgeSight for XenApp 6 Agent 5.3 (64-bit only)	x			
EdgeSight for XenApp Agent 5.3 (32- and 64-bit versions)		x	x	x

EdgeSight Server 5.3 also supports uploading data collected about system- and session-related performance for instances of XenDesktop:

Agent	XenDesktop 5.0	XenDesktop 4.0
EdgeSight for Virtual Desktops Agent 5.3	x	x

The following agent can monitor physical endpoint devices and upload the data to EdgeSight Server 5.3:

Agent	Endpoint devices
EdgeSight for Endpoints Agent 5.3	x

Agent Requirements

Agents are available for deployment on 32-bit and 64-bit machines.

EdgeSight for XenApp agent - for deployment on XenApp systems	
XenApp configuration	The target XenApp machine must meet the requirements listed in your XenApp documentation.

Other requirements	The Terminal Services service must be running to properly collect process and network data related to user sessions. (If this service is not running, process and network data cannot be associated with a session and reports dependent on this information show no data.) The session user must be a member of either the Remote Desktop users group or the Administrator users group to collect End User Experience Monitoring (EUEM) data.
--------------------	--

EdgeSight for Endpoint agent - for deployment on physical endpoint devices	
OS	Microsoft Windows XP SP2 or higher, Microsoft Windows Server 2003, Microsoft Windows Vista (Business edition or above), Windows 2008, Windows 2008 R2, or Windows 7. Both 32-bit and 64-bit systems are supported on all platforms.
CPU	500 MHz or later recommended
Memory	128 MB of RAM (256 MB recommended)
Disk	100 MB free space (25 MB of disk space for product installation and 75 MB disk space for the database)

EdgeSight for Virtual Desktops agent - to collect system-related and session-related performance data on XenDesktop 4.0 or 5.0 instances	
OS	Microsoft Windows XP SP2 or higher, Microsoft Windows Server 2003, Microsoft Windows Vista (Business edition or above), Windows 2008, Windows 2008 R2, or Windows 7. Both 32-bit and 64-bit systems are supported on all platforms.
CPU	500 MHz or later recommended
Memory	128 MB of RAM (256 MB recommended)
Disk	30 MB free space

Note: The EdgeSight for Virtual Desktops Agent is not designed to monitor the Desktop Delivery Controller (DDC) in a XenDesktop farm.

The EdgeSight agent installers check the operating system on the target machine. This helps ensure that the correct agent is installed on various devices.

- Attempts to install the Citrix EdgeSight for Endpoint agent on any system running a server operating system will result in a warning notifying you that you may be installing the wrong product. You have the option to continue installation. During a silent installation to a system running a server OS, the install fails unless the ALLOWSERVEROS property is set to 1. A message indicating the cause of installation failure is placed in the install log.

- Attempts to install the Citrix EdgeSight for Endpoint agent on a virtual desktop running XenDesktop 4.0 or higher will result in a message being displayed notifying you that you may be installing the wrong product. You have the option to continue installation. During a silent installation to a system running a XenDesktop 4.0 or higher, the install fails unless the ALLOWVIRTUAL property is set to 1. A message indicating the cause of installation failure is placed in the install log.
- Any attempt to install the Citrix EdgeSight for XenApp agent on a computer not running Terminal Server in Application Mode will fail. (Note that the agent installation does not check to ensure that the Terminal Server is properly licensed.) There is no override.

Server Requirements

The system requirements for the Citrix EdgeSight Server are listed in the following tables:

Web Server

<p>OS</p>	<p>Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 SP1 or later. Both 32-bit and 64-bit systems are supported, where available.</p> <p>Internet Information Services (IIS) 7.0 for Windows Server 2008. See "IIS 7.0 Components Required on Windows Server 2008 Systems" later in this topic for a list of specific components.</p> <p>Internet Information Services (IIS) 6.0 for Windows Server 2003</p> <p>Citrix License Server for Windows (This can be installed on a separate system; see "Citrix License Server for Windows Requirements" later in this topic for more information.)</p> <p>Microsoft Message Queuing (MSMQ), Common components only</p> <p>Microsoft .NET Framework 3.5 SP1</p> <p>Note: To support the forwarding of alerts to Microsoft® System Center Operations Manager (SCOM), the SCOM agent must be installed on the EdgeSight Web server. See "Requirements for Forwarding Alerts to System Center Operations Manager" later in this topic for more information.</p> <p>Note the following configuration requirements:</p> <p>Default Web Site running</p> <p>ASP.NET allowed in IIS</p> <p>IWAM and IUSR users active and enabled</p> <p>IIS_WPG group enabled and ASPNET user enabled (if using Windows Server 2003)</p>
<p>CPU</p>	<p>2 gigahertz (GHz) or faster CPU</p>
<p>Memory</p>	<p>2GB of RAM recommended. 512MB of RAM required.</p>
<p>Disk</p>	<p>Minimum 2 GB free space</p>
<p>Database Server</p>	

OS	Windows Server 2008 or Windows Server 2003 SP1 or later. Both 32-bit and 64-bit systems are supported on all platforms. The server edition must support SQL Server. See SQL Server Books Online for information on system requirements.
Database	<p>SQL Server 2008 (Standard or better) or SQL Server 2005 SP2 or later (Standard or better). Note that SQL Server 2008 R2 is not supported.</p> <p>Important:</p> <p>Note the following configuration requirements:</p> <p>In SQL Server 2008, the Reporting Services Role called Manage Shared Schedules no longer exists as a stand-alone role; it is now part of the System Administrator Role. For more information, see Configuring Reporting Services.</p> <p>SQL Server must be configured for case-insensitive collation. Case-sensitive collation is not currently supported for this release.</p> <p>SQL Server should be configured to use Windows Authentication or Mixed-Mode Authentication.</p> <p>Reporting Services is included with SQL Server 2008 and SQL Server 2005. Reporting Services can be installed on a separate machine from the data source.</p> <p>SQL Agent Service running and set to start automatically (if Reporting Services is installed on the machine)</p>
CPU	2 GHz or faster CPU
Memory	2GB of RAM recommended. At least 1 GB of RAM required.
Disk	Minimum 20 GB free space

Agent Database Server

The agent database server is only required if EdgeSight for Virtual Desktops Agents or EdgeSight for Endpoints Agents are used to monitor virtual desktops. The server can be installed on a physical or a virtual machine. See “Virtual Desktop Monitoring Requirements” later in this topic and [Installing EdgeSight for Monitoring Virtual Desktops](#) for more information.

OS	Windows Server 2008 or Windows Server 2003 SP1 or later.
CPU	2 GHz or faster CPU
Memory	2GB of RAM recommended. At least 1 GB of RAM required.
Disk	Typical disk space usage is generally 70 MB per virtual desktop for the databases on a single disk.

Note: The Web Server (IIS), Database Server (SQL Server), and Reporting Services can be installed on the same machine. We recommend having at least 2 CPUs in such a configuration.

IIS 7.0 Components Required on Windows Server 2008 Systems

Specific IIS 7.0 components are required on a Windows Server 2008 system which will be hosting an EdgeSight Server. These components are checked by the bootstrapper program. When configuring IIS 7.0, ensure that the following role services are selected under the Web Server role:

- Static Content
- Default Document
- ASP.NET
- ISAPI Extensions
- ISAPI Filters
- Windows Authentication
- Request Filtering
- The following Management Tools:
 - IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting
 - IIS 6 Management Console

Requirements for Monitoring Session Experience

EdgeSight for XenApp provides highly granular session experience monitoring data collected through XenApp and ICA client instrumentation. This data includes metrics on network bandwidth, ICA round trip time, and client and server startup time. Collection of these metrics depends on the following set of software components:

- EdgeSight Agent running on the Presentation Server or XenApp server
- Presentation Server 4.5 (or later) or XenApp 5.0 Enterprise or Platinum Edition
- ICA client version 10 or later

See the [Data Collection by Presentation Server or XenApp Server Version](#) for more information on data collection in relation to software component versions.

Requirements for Forwarding Alerts to System Center Operations Manager

An alert action can be configured to forward EdgeSight alerts generated from EdgeSight for XenApp agents to System Center Operations Manager (SCOM). Currently, SCOM 2007 SP1 and SCOM 2007 R2 are supported. The following software must be installed to enable the forwarding of alerts:

- The following management packs must be imported to the Operations Manager 2007 Server:
 - Citrix Library Management Pack (Citrix.Library.mp)
 - Citrix XenApp Management Pack (Citrix.PresentationServer.mp)
 - Citrix EdgeSight Management Pack (Citrix.EdgeSight.mp, provided on the Citrix EdgeSight media)
- The following software must be installed on the XenApp system being monitored:
 - EdgeSight for XenApp Agent
 - Operations Manager Agent
- The following software must be installed on the EdgeSight Server from which alerts will be forwarded:
 - Operations Manager Agent
 - Operations Manager Console or Operations Manager Authoring Console.

Currently, only alerts from by EdgeSight for XenApp agents can be forwarded. See "Configuring the Alert Action" under [Installing and Configuring Components](#) for detailed instructions on enabling alert forwarding from EdgeSight to SCOM.

Browser Requirements

EdgeSight Server Console users must have Internet Explorer version 7.0 or greater with JavaScript enabled. The following table lists software components that are required on systems from which users access the EdgeSight Server Console:

Software	Used to...
Microsoft Excel (as included with Microsoft Office 2003 or Microsoft Office 2007)	Display remote reports from the EdgeSight Server Console. Note: Ensure that Visual Basic for Applications is selected from Office Shared Features when customizing the Microsoft Excel installation.
Adobe Flash Player 10.0 or later	Display Flash-based reports and consoles. (Not currently available on 64-bit browsers.) If you do not have Flash Player installed on your system, you will be prompted to download the software.
Adobe Acrobat Reader	Display reports exported in a PDF format.

Operating System Language Support

Operating system languages must match in configurations where the EdgeSight database and Web server are installed on separate machines.

Citrix License Server for Windows Requirements

EdgeSight 5.3 requires licenses allocated from Citrix License Server for Windows 11.6. If the license server is not installed and running, license information cannot be obtained, and EdgeSight Agents are not allowed to upload data to the EdgeSight Server. You will receive instructions by email for downloading EdgeSight license keys. For documentation on licensing, including system requirements and installation instructions, see the [Citrix Licensing documentation](#).

Install the license server from the EdgeSight media (**EdgeSight Component Installers > Install Citrix Licensing**). The license server can be installed on the same system as the EdgeSight Web server, or it can be installed on another system, as long as it is accessible by the Web server. The license server can be shared by multiple EdgeSight servers.

Important: If you are installing the License Management Console and EdgeSight Server on the same machine, install EdgeSight Server first. Installing the License Management Console precludes access to the EdgeSight Server web site. Also, if there is a firewall between the license server and the computers running EdgeSight components, you must specify a static Citrix Vendor Daemon Port number on the license server.

When installing the license server, accept the defaults provided by the MSI file for the destination folder and the license file location. When selecting features, you can choose whether to select the License Management Console; this feature is not required, but may be useful in managing your licenses.

Additional Requirements for Monitoring Citrix License Servers

The License Server Monitoring feature is designed to monitor Citrix License Server for Windows 11.5, 11.6, or 11.6.1. The feature is not dependent on the EdgeSight agents, because license servers are polled directly by EdgeSight Server. License servers must be explicitly identified using the EdgeSight Server Console before they are monitored for license type, usage, and availability.

Active Application Monitoring Requirements

The system requirements for systems running the EdgeSight Active Application Monitoring Controller and Launcher are listed in the following table.

Controller and Launcher Requirements

OS	<p>Controller</p> <p>Microsoft Windows Vista, Microsoft Windows XP, Microsoft Windows 7, Microsoft Windows Server 2003, Microsoft Windows Server 2008, and Microsoft Windows Server 2008 R2 (32-bit and 64-bit systems on all operating systems)</p> <p>Launcher</p> <p>Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows Server 2003 (32-bit systems only), Microsoft Windows Server 2008, and Microsoft Windows Server 2008 R2 (32-bit and 64-bit systems on all operating systems except as noted)</p> <p>ICA Client Version 10 or higher</p> <p>Citrix Presentation Server 4.0 or higher, Citrix XenApp 5.0 or 6.0</p> <p>.NET Framework 2.0 or later is required for all Launchers and Controllers that will be establishing connections using the Web Interface.</p> <p>Visual J# Version 2.0 (if using XML Interface Connector)</p> <p>Citrix EdgeSight for XenApp Agent, Advanced Mode, must be installed on the server under test. If a Basic mode agent is installed, application response alerts will not be generated and no data will be displayed in application response reports.</p>
CPU	2 gigahertz (GHz) or faster CPU
Memory	1 gigabyte (GB) of RAM
Disk	Minimum 200 megabytes (MB) of free space

Virtual Desktop Monitoring Requirements

You can use EdgeSight to monitor virtual desktops. The following tables list software components used in such an environment. (As with any EdgeSight deployment, you will also need SQL Server Reporting Services and Citrix License Server for Windows, as specified in this document.) For instructions on installing the EdgeSight components in a virtual desktop environment, see Chapter 4, “Installing EdgeSight for Monitoring Virtual Desktops.”

When monitoring virtual desktops running XenDesktop 4.0 or later, the following software components must be in place.

System Requirements for EdgeSight 5.3

Software Component	For more installation information...
XenDesktop 4.0 or 5.0	XenDesktop 4 System Requirements XenDesktop 5 System Requirements XenDesktop 4 (installation information is under "XenDesktop 4 Service Pack 1" and "Administering XenDesktop") Installing and Setting up XenDesktop 5
EdgeSight Server 5.2 or later	Installing EdgeSight Server
EdgeSight for Virtual Desktops Agent 5.2 or later	Installing EdgeSight for Monitoring Virtual Desktops
EdgeSight Agent Database Server 5.2 or later	Installing EdgeSight for Monitoring Virtual Desktops

Install and Configure

Preparing to Install Citrix EdgeSight

Citrix® EdgeSight™ software includes the following components:

- EdgeSight Server—Displays performance data for monitored devices
- EdgeSight for XenApp Agent—Monitors the performance of XenApp and Presentation Server systems. Multiple versions of the agent are provided to accommodate different XenApp versions.
- EdgeSight for Endpoints Agent—Monitors the performance of physical clients and XenDesktop 3.0 instances
- EdgeSight for Virtual Desktops Agent—Monitors the performance of XenDesktop 4.0 instances. This agent enables the following features:
 - Collection of ICA channel data including XenDesktop multi-media counters
 - Collection of End User Experience metrics
 - Alerting on XenDesktop session performance
- EdgeSight Agent Database Server—Stores performance data for agents monitoring virtual desktops
- EdgeSight Active Application Monitoring Components—Performs automated testing to monitor the end user experience of applications in XenApp and Presentation Server environments

Citrix EdgeSight software is installed using Windows Installer (MSI) files. The EdgeSight Server MSI files are invoked using a bootstrapper program (setup.exe). The following table lists the MSI files by EdgeSight component. Separate MSI files are provided for 32-bit and 64-bit systems for EdgeSight Server and EdgeSight Agents.

EdgeSight Component	MSI Name
EdgeSight Server (32-bit systems)	EdgeSightServer.msi
EdgeSight Server (64-bit systems)	EdgeSightServerx64.msi
EdgeSight for XenApp Agent (32-bit systems)	EdgeSightXAAgent.msi
EdgeSight for XenApp Agent (64-bit systems)	EdgeSightXAAgentx64.msi
EdgeSight for XenApp Agent for XenApp 6 (64-bit systems)	EdgeSightXA6Agentx64.msi
EdgeSight for Endpoints Agent (32-bit systems)	EdgeSightEPAgent.msi

EdgeSight for Endpoints Agent (64-bit systems)	EdgeSightEPAgentx64.msi
EdgeSight for Virtual Desktops Agent (32-bit systems)	EdgeSightVDAAgent.msi
EdgeSight for Virtual Desktops Agent (64-bit systems)	EdgeSightVDAAgentx64.msi
EdgeSight Agent Database Server	EdgeSightAgentDBS.msi
EdgeSight Active Application Monitoring components (Controller, Launcher, and Web Interface)	EdgeSight Active Application Monitoring.msi
Citrix License Server	CTX_Licensing.msi

Note:

Note: Do not modify the base MSI files. Modifying the base MSI files can interfere with support efforts in case of installation issues. You can customize the installation by specifying options and properties on the command line or by creating a transform.

The EdgeSight 5.3 media contains the 5.2 SP1 releases of the EdgeSight for XenApp, EdgeSight for Endpoints, and EdgeSight for Virtual Desktops agents. New EdgeSight 5.3 agents are now available for download from the Citrix Downloads page at: <http://www.citrix.com/English/ss/downloads/index.asp>.

Important: EdgeSight 5.3 agents should be installed whenever possible because they include important fixes and enhancements. EdgeSight 5.2 SP1 agents should only be installed in the following cases:

- For use with an EdgeSight Server which is still at version 5.2
- If other 5.2 SP1 agents are installed and you want to keep all agents at the same version for maintainability reasons

Server Installation Overview

Use setup.exe to install an EdgeSight Web server and database server. After you install and configure the server components, deploy the applicable EdgeSight Agent to XenApp Servers, end-user systems, and virtual desktops. In addition to the software listed in “Server Requirements” in [System Requirements](#), EdgeSight Server requires the following software. It is highly recommended that you install the following software before installing EdgeSight Server software.

- **Microsoft SQL Server Reporting Services**—required for the generation of historical reports. Reporting Services must be in place before reports can be generated and displayed. For information on configuring Reporting Services for use with EdgeSight software, see [Configuring Reporting Services](#).
- **Citrix License Server for Windows 11.6 or later**—used to supply a license authorizing the agent to upload data to a Citrix EdgeSight Server. The license server can be installed anywhere on the network and can be shared by multiple EdgeSight servers. The license server and EdgeSight license files must be in place before data can be uploaded to the server. A Citrix License Server MSI is included with the EdgeSight media for your convenience. For more information, see “Citrix License Server for Windows

Requirements” in [System Requirements](#).

When planning your installation, the required server components can be installed on separate physical machines. (The Web server can be installed on the same machine as the database server, but the machine should have at least two processors.) In all cases, ensure that the machines have sufficient memory and processor capabilities (as described in “Server Requirements” in [System Requirements](#)) and that the machines are in the same domain.

The MSI file installs server files for both EdgeSight for XenApp and EdgeSight for Endpoints. Both products use the same underlying server technologies. You can enable or disable agent support for either product after installation.

Note: EdgeSight Server should not be installed on the same system as XenApp in a production environment, but this can be done to support a proof of concept environment.

Agent Deployment and Installation Overview

Use the applicable EdgeSight Agents MSI file to install EdgeSight agents on target machines. Separate MSI files are provided for each type of agent (EdgeSight for XenApp, EdgeSight for Virtual Desktops, and EdgeSight for Endpoints), for each target system architecture (32-bit and 64-bit), and for XenApp versions (Presentation Server / XenApp 5 and XenApp 6). The EdgeSight for XenApp Agent MSI file provides both the Basic and Advanced versions of the agent. You can deploy agents to end-user systems or XenApp Servers in your enterprise using several methods:

- Direct command-line or GUI-based installations using the MSI file.
- Define an Active Directory Group Policy Object for software distribution of the MSI file. Note that GPO push to users is supported.
- Perform a System Management Server (SMS) issuance of the MSI file.

If you are installing the EdgeSight for Endpoints agent or the EdgeSight for Virtual Desktops agent on virtual desktops, additional software components and installation tasks are required, as described in [Installing EdgeSight for Monitoring Virtual Desktops](#). Discuss your software deployment environment with your Sales Representative; they can assist you in implementing an effective means of deploying the agent.

Active Application Monitoring Installation Overview

EdgeSight Active Application Monitoring is an automated performance testing tool that periodically samples critical application transactions to monitor the availability and responsiveness of virtualized applications, providing insight into application performance and end-user experience.

EdgeSight Active Application Monitoring software includes the following components:

- Citrix EdgeSight Controller—used to record and create virtual user scripts and define tests. When the test is ready for playback, the Controller instructs the Launchers to run the test for a specific period of time.

- **Citrix EdgeSight Launcher**—receives commands from the Controller and generates virtual user ICA sessions on the target Presentation Servers and XenApp servers. The number of Launchers required will vary based on the target virtual user load.
- **Web Interface Connector**—allows users to connect to applications made available through the XML Service. This feature requires the Visual J# Version 2.0 Redistributable Package available from Microsoft.

Launchers are installed on clients of the Servers that will be under test. They can be installed on systems with the Controller and as stand-alone launchers. See [Installing EdgeSight Active Application Monitoring Software](#) for installation procedures for these components.

Pre-Installation Considerations

Software running in your environment may need to be configured to allow Citrix EdgeSight software to operate properly. Review the following considerations and related actions and determine if they apply to your environment. Also, review the readme file for additional release-specific requirements.

Agent

- **Proxy Servers and Settings**—If the EdgeSight Agent will communicate with the EdgeSight Server through a proxy server, ensure that you have the proxy server IP address, port number, and credentials required prior to installing EdgeSight Agent. See [Installing EdgeSight Agents](#) for instructions on specifying proxy server information during agent installation.
- **Firewalls**—If firewall software is resident on machines on which EdgeSight Agents will be installed, the listen port on the client machine (port 9035) must be open. This is the port on which the agent listens for remote connections from the browser displaying the EdgeSight console. There is an option during agent installation to automatically set a Windows Firewall exception for the listen port if the firewall is running (enabled or disabled). See [Installing an Agent Using the User Interface](#) for instructions on specifying the listen port number. Also see “Configuring Firewalls” in [Configuring Third Party Software](#) for information relating to personal firewalls.
- **Virus scanning software**—If your environment uses virus scanning software, script blocking features must be disabled to allow the EdgeSight Agent to run scripts. Also, exclude agent data files from being scanned. See “Configuring Antivirus Software” in [Configuring Third Party Software](#) for detailed information on which files should be excluded from scans.

Server

- **Virus scanning software**—If your environment uses virus scanning software, script blocking features must be disabled to allow EdgeSight Server to run scripts. Also, exclude the server database from being scanned. See “Configuring Antivirus Software” in [Configuring Third Party Software](#) for detailed information on which files should be excluded from scans.
- **IIS Security Lockdown template**—Any IIS Security Lockdown templates must allow the IIS components listed in “Server Requirements” in [System Requirements](#) to run. Adjust the template as required.

- **Group Policy**—Ensure that Group Policies do not prohibit any of the required software components from running on your EdgeSight Server. Also, ensure that policy changes that would prohibit software components from running are not scheduled for deployment after the installation is complete.
- **SQL Server 2005 Password Policy**—SQL Server 2005 includes an option to enforce Windows password policy. This option is enabled by default and will cause an error if the passwords supplied for accounts during installation do not meet the necessary strength requirements. If an error occurs containing the text, “Password validation failed. The password does not meet Windows policy requirements because it is not complex enough,” then double check your password requirements, reattempt installation, and supply appropriately complex passwords.
- **SSL Certificate**—If you choose to enable SSL for use on the Citrix EdgeSight Web server, you must either use an SSL certificate from a recognized certificate authority or a correctly generated and installed certificate from Microsoft Certificate Server to allow proper software operation. For detailed information, see [How to Configure EdgeSight to use SSL with Microsoft Certificate Services](#). SSL certificates which do not meet these criteria do not allow remote pages to be displayed or remote scripts to be run. Attempts to perform these actions without a valid certificate result in an error message.
- **SMTP Server**—During installation, you must specify an SMTP server. It is important that a valid SMTP server name is used. EdgeSight Server uses the SMTP server for many operations, including the distribution of alert notifications, server error conditions, and new user passwords.

Installing EdgeSight Server

The server installation is launched using the setup.exe bootstrapper. The installation will fail if the server MSI file is invoked directly.

The preferred method of installing EdgeSight Server is to use the bootstrapper and perform the installation using the Citrix EdgeSight Installer user interface. This method offers typical and custom installation options. A typical installation offers only the minimum set of properties required for installation. A custom installation offers the same set of public properties as a command-line installation.

If required, you can perform a command-line installation using the msiexec command. You must specify public properties to define installation settings. Review [Installing EdgeSight Server Using the Command Line](#) for a description of installation properties.

If you are upgrading, see [Upgrading or Uninstalling EdgeSight Server](#) for more information.

If you are monitoring endpoint devices, download EdgeSight for Endpoints license files (CES_*.lic), then manually place them in the MyFiles folder of the license server directory, for example: %ProgramFiles%\Citrix\Licensing\MyFiles. These files will need to be in place prior to running the post-installation wizard.

Prerequisite Checking

The bootstrapper performs checks for the following software prerequisites and system characteristics. The conditions checked can be required or recommended. If any of the required conditions is not met, the installation stops. Correct the condition and restart the installation. Recommended conditions are flagged with a warning, but installation can continue at the discretion of the installer.

Condition	Required
.NET Framework 3.5 SP1	Yes
Windows Server 2003 or Windows Server 2008	Yes
Internet Information Services (IIS) 6.0 or later. See “IIS 7.0 Components Required on Windows Server 2008 Systems” in System Requirements for information specific to IIS 7.0 and Windows Server 2008.	Yes
Microsoft Message Queuing (MSMQ). The MSMQ service must be running.	Yes
SQL Server 2005 SP1 or later (Standard or better). This can be on a different machine from where the installation is being run.	Yes

512 megabytes (MB) of RAM

Note that 2GB is recommended.

No. Installation can continue, but performance may be affected.

Note that some requirements for full operation, such as Citrix License Server for Windows and SQL Server Reporting Services, are not checked by the bootstrapper.

Installing EdgeSight Server Using the User Interface

Before performing an EdgeSight Server installation, set up a “run as” account for EdgeSight. You will need to supply the account username and password during server installation. Specify the account using the computer name and username (*computername\username*) or the domain name and username (*domainname\username*). Do not use a fully qualified domain name (FQDN), as this will result in an installer error.

Note that not all public installation properties are exposed when performing a typical installation using the user interface. Properties not explicitly set from the user interface are set to their default value if one exists. However, performing a custom installation will expose all available properties. The following procedure is based on a custom installation. To install a server using the user interface:

1. Insert the media or run Autorun.
2. Select **EdgeSight Server** to display the Choose Language dialog.
3. Select the language for the installation and click **Continue** to display the Welcome screen.
4. Click **Next** to continue to display the Select Features screen.
5. Select the applicable radio button for the EdgeSight Server components to be installed. You can install a Web server and database, or just a database. In both cases, if there is an existing database, it will be upgraded as necessary. Click **Next** to continue to display the Prerequisite Check screen.
6. A check for minimum requirements is performed and the result of the check is displayed. If minimum requirements are not met, the installation is stopped and you are notified of missing components. If minimum requirements are met, but limitations are present due to the configuration of the target system, warnings are displayed. (Examples of warning conditions are the not meeting minimum memory requirements.) You can continue the installation even though warnings have been issued. Click **Next** to display the End-User License Agreement screen.
7. After reading the license, select the **I accept** radio button and click **Next** to display the Choose Setup Type screen.
8. Select the applicable radio button for the type of setup to be performed (Typical or Custom). In this case, choose the **Custom** radio button and click **Next** to display the Database Server screen.
9. Select an existing server name from the list or enter a server name. The name of the machine on which you are running the installer is preloaded into the entry field. You can also enter a named instance in this field (*servername\instancename*).
10. Select an authentication method. The method you choose is partially determined by the accounts set up when SQL Server was installed. (Note that you must have administrative

privileges on the database server.) Click the **Test Connect** button to test the connection to the SQL Server. Click **Next** to display the next Database Information page.

11. Select the **Install a new EdgeSight database** radio button to create a new database. (If you were performing an upgrade, you would select the applicable radio button and choose an existing database from the list.)
12. Enter a name for the new database and click **Next** to display the Database User Information screen.

Database names must be unique within an instance of SQL Server and comply with the rules for identifiers. Also, the database name can not contain hyphens, the pipe character (|), single quotes, a period (.), or spaces.

For information on identifiers, see SQL Server Books Online for your version of SQL Server.

13. Enter and confirm the account username and password that the Web server uses when connecting to the database. If you are performing the installation using local machine accounts, enter the computer name and username (*computername\username*). If you are performing the installation using domain accounts, enter the domain name and username (*domainname\username*). Do not supply a fully qualified domain name, as this will result in an installer error.
14. Click **Validate** to test the user credentials. After the credentials have been successfully validated, click **Next** to display the Database Properties screen.
15. Configure the database properties as follows:
 - **File Group Size**—Accept the default file size or enter a new file size. Each of the eight files in the file group is created using the specified size. The default value is sufficient space for most installations. A smaller size may be selected for pilot installations.
 - **Log File Size**— Accept the default log file initial size or enter a new file size. The default value is sufficient space for most installations.
 - **Recovery Model Options**—Select a database recovery model (Simple, Bulk-logged, or Full) from the drop-down menu. The default recovery model is Simple. If the recovery model is changed to Full, ensure that a database backup strategy is in place to effectively manage database size. See SQL Server Books Online for more information on recovery models.

Note: The installer uses the default file group and log file creations as configured in the SQL Server installations. A SQL Server administrator can change the location of the file groups and log files, but the SQL Server service must be restarted before the new locations will take effect.

16. Click **Next** to display the Server Location screen.
17. Review the default values for the program files root and the data files path. You can accept the default values or click the **Browse** button to select a different location for the files. To display information about space availability on all system drives, click the **Disk Usage** button. When you have specified server file locations, click **Next** to display the Ready to Install screen.

18. Click **Install** to begin the installation. (If you need to review or change any settings before installing, use the **Back** button to return to the configuration screens.) Installation status is displayed while the installation is being performed. When the installation is finished, the Complete screen is displayed.
19. The checkbox indicating you want to go to the EdgeSight Server Website (<http://servername:port/edgesight/app/suilogin.aspx>) is checked by default. You must go to the Website to perform initial configuration tasks, as described in [Running the Post-Installation Setup Wizard](#). (If you want to perform initial configuration at a later time, deselect the checkbox. However, it is recommended that you complete initial configuration directly after completing the installation.) Click **Finish** to exit the installer.

Note: You will need to communicate with the license server during the initial configuration procedure. If you have not installed the license server, deselect the checkbox, close the installer, install the license server, and then log into the Web site.

Installing EdgeSight Server Using the Command Line

The MSI file uses public properties to specify custom install settings. You can edit public properties using the following methods:

- Run the installer user interface (if the property is exposed). A log file is not created when the user interface is used for installation.
- Create a transform file using a tool such as Orca. For more information on using Orca with MSI files, see <http://support.microsoft.com/kb/255905>.
- Specify key/value pairs on the command line. This method allows you to control the full range of installation options, including specifying a log file, as well as being able to specify public properties. The syntax for key/value pairs is *KEY=value*.

See your MSI documentation for syntax rules for property values. The following table lists the public properties available when installing the Citrix EdgeSight Server. You only need to specify properties with default values if you want to specify a value other than the default. Also, whether some properties are specified depends on what other properties are being specified. For example, if Windows authentication is not enabled using the `WINDOWS_AUTH` property, the `DBUSERNAME` and `DBPASSWORD` properties must be defined.

Note: Although additional properties are exposed when you examine the MSI file, only the public properties listed in the following table should be explicitly specified.

Property Name	Description
<code>PREREQUISITES_PASSED</code>	If this property is specified with any value, the bootstrapper is bypassed and you are allowed to perform a command-line installation of the server.
<code>DATABASEOPTIONS</code>	Specifies whether to install a new Citrix EdgeSight database or upgrade an existing database. Valid values are <code>new</code> or <code>upgrade</code> ; the default value is <code>new</code> .
<code>DATABASESERVER</code>	The name of the server running an existing Citrix EdgeSight database. It is not necessary to specify a value when running the database locally.
<code>DBUSERNAME</code>	The username for the SA user. It is not necessary to specify a value if Windows authentication is enabled (<code>WINDOWS_AUTH=1</code>).
<code>DBPASSWORD</code>	The password for the SA user. It is not necessary to specify a value if Windows authentication is enabled (<code>WINDOWS_AUTH=1</code>).

WINDOWS_AUTH	<p>Specifies whether to use Windows authentication. Valid values are 1 (use Windows authentication) or 0 (do not use Windows authentication); the default value is 1.</p> <p>Note: If Windows authentication is not used, the DBUSERNAME and DBPASSWORD properties must be defined.</p>
DBNAME	<p>The name of the Citrix EdgeSight database that will be created during installation. Database names must be unique within an instance of SQL Server and comply with the rules for identifiers. Also, the database name can not contain the pipe character (), single quotes, a period (.), a hyphen (-), or spaces. For information on identifiers, see SQL Server Books Online for the your version of SQL Server. The default value is EdgeSight.</p>
ACCOUNTNAME	<p>The account name for the EdgeSight “run as” account. Specify the account using the computer name and username (<i>computername\username</i>) or the domain name and username (<i>domainname\username</i>). Do not use an FQDN.</p>
ACCOUNTPASSWORD	<p>The password for the EdgeSight “run as” account.</p>
DATAFILESIZE	<p>Specifies the initial size in megabytes of a data file. Each of the eight files in the file group is created using the specified size. The default value is 500 and is sufficient for most installations.</p>
LOGFILESIZE	<p>Specifies the initial size in megabytes of the log file. The default value is 500 and is sufficient for most installations.</p>
RECOVERYMODEL	<p>Specifies the database recovery model. Valid values are FULL, SIMPLE, and BULK_LOGGED; the default value is SIMPLE.</p>
DATADIR	<p>EdgeSight Server uses temporary files for storing data uploads from agents, including crash reports. The default directory is %ProgramFiles%\Citrix\System Monitoring\Server\EdgeSight\Data. Because there may be significant file growth in this directory, it may be desirable to locate this directory on a separate drive or partition.</p> <p>Note: The data directory cannot be on a mapped drive.</p>
EDGEDIR	<p>Contains the web pages, scripts, .Net components and other components that make up the EdgeSight Server Web site. The default value is %ProgramFiles%\Citrix\System Monitoring\.</p>
INSTALLOPTIONS	<p>Specifies which components are to be installed. Set the value to <i>full</i> to install the database, Web server, and script handler components. Set the value to <i>dbonly</i> to install only the database component.</p>

Use the msixec command to install the server using the command-line interface. Public properties are specified as *KEY=value* pairs. Note that path names must be enclosed in quotes. The following is a sample msixec command line:

```
Msixec /i EdgeSightServer.msi /l*v logfile.log /qn
PREREQUISITES_PASSED=1 WINDOWS_AUTH=1
```

```
ACCOUNTNAME=mydomain\myaccount ACCOUNTPASSWORD=mypass  
DBNAME=EdgeSight50  
DATADIR="D:\Citrix\System Monitoring\Data"
```

The `/i` flag is used to specify the package being installed. The `/l*v` flag is used to specify the installation log file name. (Capturing a verbose installation log is strongly recommended.) Use the `/qn` (quiet) flag to install an agent with no user interaction. For a complete list of standard MSI command-line arguments, open a Command Prompt window and type `msiexec /h` to invoke help, or refer to *The Command-Line Options for the Microsoft Windows Installer Tool Msiexec.exe* at <http://support.microsoft.com/kb/314881>.

Running the Post-Installation Setup Wizard

After you have completed the Citrix EdgeSight Server installation, you must use the Citrix EdgeSight Post-Installation Setup Wizard to perform initial server configuration. The wizard is displayed the first time you log into the EdgeSight Server Web site (<http://servername:port/edgesight/app/suilogin.aspx>). The post-installation wizard helps you perform the following tasks:

- Create a company. A company is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies.
- Create the Superuser account. This account has access to all companies hosted on the server and can create other users.
- Configure email settings. This information is used on notification emails generated by the server.
- Configure agent support.
- Configure licensing if EdgeSight for Endpoint agent support is enabled.

To configure your Citrix EdgeSight Server:

1. Review the tasks you will perform and ensure that you have the information at hand to specify the settings listed above. Click **Next** to display the Create an Initial Company page.
2. Enter a name for the company for which data will be displayed on the Web site.
3. Select a time zone from the drop-down menu to be used by the server when displaying the time and triggering jobs. There is a single time zone for each company defined on a Citrix EdgeSight Server. All data for that company is aggregated based on the day boundary for that time zone. This ensures greater data consistency when agent machines are in a number of different time zones.
4. Select the default display language for new user accounts from the drop-down menu. Click **Next** to display the Create the Superuser Account page.
5. Enter login information for the Superuser account (a universal login ID to be used by the Citrix EdgeSight administrators). This login enables administrators to access data from all companies and perform server administrative tasks. The Superuser account cannot be deleted. Enter a first and last name, a login ID in the form of an email address, and a password. You must confirm the password. Click **Next** to display the Configure Email Settings page.
6. Enter the name of the SMTP server used to route email. The SMTP server can be running locally or remotely.

7. Enter the email address for the person or group who should be notified of important events occurring on the Web site. In most cases, this person is the Citrix EdgeSight Administrator.
8. Enter a display name and email address to be used when email is generated by the Web site. (Once the Web server is installed, you use the EdgeSight Server Console to determine additional criteria for email notifications.) Click **Next** to display the Configure Agent Support and Licensing page.
9. Select which types of agents, if any, to display on the server from the support drop-down menus. (For example, if the EdgeSight server will only be used to monitor XenApp systems, disabling display support for the other types of agents can provide a more streamlined interface. Similarly, if the EdgeSight Server will only be used for license server monitoring, you can disable support for all agents.) EdgeSight provides the following types of agents:

EdgeSight for XenApp, Basic—Basic agents require only that you have a XenApp Enterprise license available on your Citrix Licensing Server.

EdgeSight for XenApp, Advanced—Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix Licensing Server.

EdgeSight for Endpoints—Endpoint agents provide monitoring and data collection for endpoint devices.

EdgeSight for XenDesktop—EdgeSight for Virtual Desktops agents provide monitoring and data collection for XenDesktop devices.

Note: This setting only determines whether reports and administrative pages are displayed on the console; data continues to be collected, uploaded, and stored even if you have disabled display support. You can change the agent display support at any time after installation using the EdgeSight Server Console.

10. Enter the license server name and port number used for communication with the license server which will supply EdgeSight for Endpoints Agent licenses. The license server can be installed on the machine hosting the EdgeSight Web server, or can be installed on another machine as long as it is accessible via the network. (EdgeSight for XenApp Agents obtain their licenses directly from the license server without intervention from EdgeSight Server. They use the license server specified in their agent configuration. See [Managing Licenses](#) for more information on licensing.)
11. This step is optional. After entering the license server name and port, click the **Test License Server** button to ensure that you can connect to the specified license server and that EdgeSight licenses are found. If the test is successful, a success message is displayed, along with the type and number of EdgeSight licenses installed. The test can fail because the license server is not accessible, or because the license server is not the correct version. Verify the license server name and port, or upgrade the license server and retry the test. You may also want to try using the IP address or FQDN of the license server.
12. Click **Next** to display the Review Citrix EdgeSight Server Settings page.
13. Review the selected configuration settings. Use the **Back** button to return to previous pages and adjust settings. When you are satisfied with the settings, return to the review screen and click **Finish** to save the configuration. The Citrix EdgeSight login

page is displayed if the checkbox for this option is selected.

Installing EdgeSight Agents

In most production environments, the agent is deployed and installed as described in “Agent Deployment and Installation Overview” in [Install and Configure](#). You can also perform an agent installation on a single client system. You may want to use this method during evaluation or when deploying and installing small numbers of clients.

If you are deploying agents for monitoring virtual desktops, see [Installing EdgeSight for Monitoring Virtual Desktops](#) for information specific to that environment.

Note: Whatever deployment and installation methods you choose, you must have administrator privileges on the target machines.

Agent Mode

The EdgeSight for XenApp Agent has two modes of operation, Basic and Advanced:

- Basic agents require only that you have a XenApp Enterprise license available on your Citrix Licensing Server.
- Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix Licensing Server.

When an EdgeSight for XenApp Agent is installed on a XenApp or Presentation Server machine, the agent mode enabled by default depends on the version and edition of XenApp or Presentation Server. The following table shows the default agent mode by XenApp and Presentation Server version and edition. The table also shows whether the **Mode** tab is displayed on the Citrix System Monitoring Agent control panel applet.

XenApp or Presentation Server Version	XenApp or Presentation Server Edition	Default Agent Mode	Mode Tab Available
6.0	Platinum	Advanced	No
6.0	Enterprise	Basic	Yes
5.0	Platinum	Advanced	No
5.0	Enterprise	Basic	Yes
4.5	Platinum	Advanced	No
4.5	Advanced/Standard	Advanced	No
4.5	Enterprise	Basic	Yes
4.0	Platinum	Advanced	No

4.0	Advanced/Standard	Advanced	No
4.0	Enterprise	Basic	Yes

Software Configuration Tasks

You may need to change the configuration of some software, such as antivirus software or personal firewalls, on machines which will run the EdgeSight Agent to ensure proper operation. You can perform these configuration tasks before or after installing the EdgeSight Agent. For more information, see [Configuring Third Party Software](#).

Antivirus Configuration Checking

Due to the manner in which buffer overflow protection was implemented in McAfee VirusScan 8 or 8i with Patch 10, this feature may conflict with the operation of the EdgeSight Agent. (In later versions of McAfee VirusScan, this feature was implemented differently and does not conflict with EdgeSight Agent operation.) The EdgeSight Agent installer checks for McAfee 8 or 8i with Patch 10 or below on the target machine. If the EntApi.dll file is present with version 8.0.0.277 and below, the installation exits with an error. The check is performed on both full UI and unattended installations. In a command-line installation, the check can be omitted from the installation process by specifying the `OVERWRITE_COMPCHECK` property with a value of 1.

Note: The `OVERWRITE_COMPCHECK` property should only be used if you disable the McAfee buffer overflow protection feature as described under "Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent" in the [Known Issues in EdgeSight 5.3](#).

Installing an Agent Using the User Interface

Note that not all public installation properties are exposed when installing using the user interface. Properties not explicitly set from the user interface are set to their default value if one exists. To install an agent using the user interface:

1. Insert the media.
2. Select **EdgeSight Agent Installers**.
3. Select the agent type to be installed to display the Welcome screen.
4. Click **Next** to display the License Agreement screen.
5. After reading the license, select the **I accept** radio button and click **Next** to display the Company Information screen.
6. Enter the company name. This should match the company name specified during EdgeSight Server setup.

If you are installing the agent on an endpoint device, enter the department name. If no department name is provided, the agent data will be displayed under the root department.

If you are installing the agent on XenApp, select the operational mode from the **Mode** drop-down menu. If you choose **Basic** mode, some capabilities are not available and no EdgeSight license is consumed. Basic mode is used when installing an EdgeSight for XenApp agent on an Enterprise Edition system.

Click **Next** to display the Agent Location screen.

7. Enter the installation path for the agent or accept the default value. You can browse to select a non-default location.
8. Enter the installation path for the data files or accept the default. You can browse to select a non-default location. Click **Next** to display the Network Settings screen.
9. Enter the server name and port number. These are required fields.
10. The **Automatically configure Windows Firewall for Port 9035** checkbox is selected by default. Enabling this feature automatically configures the firewall for the listen port (the port on which the agent listens for remote connections from the browser displaying the EdgeSight Server console). The firewall must be running, but can either be enabled or disabled. The exclusion is set up for Domain networks. If an exception for Private networks is required, the Domain exception can be used as a template. If you do not want Windows Firewall automatically configured, deselect the checkbox.
11. If an SSL network connection is required, select the **Use SSL** checkbox. (This is equivalent to setting the CONNECTION_FLAGS property.)

12. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server. (This is equivalent to setting the PROXY_ADDRESS, PROXY_PORT, and PASSWORD properties.) Click **Next** to display the Advanced Settings screen.
13. The Advanced Settings screen is only used if you are installing the EdgeSight for Endpoints agent or the EdgeSight for Virtual Desktops agent on virtual desktops in a pool. See [Installing EdgeSight for Monitoring Virtual Desktops](#) for instructions on installing and deploying agents in this type of environment. Click **Next** to display the Ready to Install screen.
14. Click **Install** to begin the installation. (If you need to review or change any settings before installing, use the **Back** button to return to the configuration screens.) When the installation is complete, the Setup Complete screen is displayed.
15. Click **Finish** to complete the installation. The Installer Information dialog is displayed, prompting you to reboot your system so that configuration changes will be applied.
16. Click **Yes** to reboot your machine.

Installing EdgeSight Agents Using the Command Line

The MSI file uses public properties to specify custom install settings. You can edit public properties using the following methods:

- Run the installer user interface (if the property is exposed). This method offers fewer installation options than using the command-line interface. Also, a log file is not created when the user interface is used for installation.
- Create a transform file using a tool such as Orca.
- Specify key/value pairs on the command line. This method allows you to control the full range of installation options, including specifying a log file, as well as being able to specify public properties. The syntax for key/value pairs is *KEY=value*.

See your MSI documentation for syntax rules for property values. The following table lists the public properties used when installing the EdgeSight agent:

Property Name	Description
COMPANY	The company under which data will be displayed on EdgeSight Server. If this property is not specified, the server considers the device unmanaged, and the agent cannot upload data to the server.
DEPARTMENT	The department under which data will be displayed on EdgeSight Server. Special characters are not allowed in the name of an EdgeSight department. If this property is not specified, the device is assigned to the default root department. Note: This property is only available for EdgeSight for Endpoints agents; EdgeSight for Virtual Desktops agents and EdgeSight for XenApp agents use the Farm structure as the department structure.
INSTALLROOT	Location of the main Citrix EdgeSight directory. For example: INSTALLROOT="%programfiles%\citrix\system monitoring\Agent"

DATA_DIR	<p>Location of the Citrix EdgeSight data directory, within quotation marks. If this property is not specified, data files are placed in the default location:</p> <p>%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data\</p> <p>On Microsoft Vista systems, the default path is:</p> <p>%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\</p> <p>Note that the data directory cannot be on a mapped drive.</p>
DELETE_DATA_ON_UNINSTALL	<p>Controls whether agent data files (database and log files) are deleted when the agent is uninstalled.</p> <p>0 = Do not delete files on uninstall</p> <p>1 = Delete files on uninstall</p> <p>Default value is 1.</p>
REMOTE_SECURITY	<p>Determines whether security is enabled for remote connections from the server.</p> <p>0 = Security disabled</p> <p>1 = Security enabled</p> <p>Default value is 1.</p> <p>See the REMOTE_SECURITY_GROUP property for more information on remote device security.</p> <p>Note: This option is deprecated and will be removed in a future version.</p>

<p>REMOTE_SECURITY_GROUP</p>	<p>Local machine group to which the current working user must belong for remote connections from the server. Note that it is the current working user of the machine that is checked, not the user account used to log into the Citrix EdgeSight Server Console.</p> <p>The REMOTE_SECURITY and REMOTE_SECURITY_GROUP properties work together to determine the level of security for remote device access as follows:</p> <p>RemoteSecurity=1, RemoteSecurityGroup=<not set></p> <p>This is the most secure and restrictive setting. In order to display real-time reports based on the agent database, the EdgeSight Server Console user must be a local administrator on the actual device.</p> <p>RemoteSecurity=1, RemoteSecurityGroup=<Active Directory group></p> <p>An Active Directory group must exist or be set up in order to use the REMOTE_SECURITY_GROUP property. Add all EdgeSight users to this group who need access to the real-time reports. This approach allows you to carefully control those users with access to real-time reports.</p> <p>RemoteSecurity=0, RemoteSecurityGroup=<any value></p> <p>This is the least secure setting. This gives all EdgeSight Server Console users the ability to display real-time reports. This setting is generally not recommended.</p>
<p>SYNCH_AD_TREE</p>	<p>Determines whether to synchronize the Active Directory tree with the Citrix EdgeSight department tree.</p> <p>0 = Synchronization disabled</p> <p>1 = Synchronization enabled</p> <p>Default value is 0.</p>

<p>ALLOWSERVEROS</p>	<p>Determine whether to allow an EdgeSight for Endpoints agent to be installed on a system running a server OS.</p> <p>0=No installation on server OS</p> <p>1=Install on server OS</p> <p>Default value is 0.</p> <p>Note: During a silent installation of an EdgeSight for Endpoints agent on a system running a server OS, the install fails unless the ALLOWSERVEROS property is set to 1.</p>
<p>ALLOWVIRTUAL</p>	<p>Determine whether to allow an EdgeSight for Endpoints agent to be installed silently on XenDesktop 4.0 instances.</p> <p>0=No installation on XenDesktop 4.0 instance</p> <p>1=Install on XenDesktop 4.0 instance</p> <p>Default value is 0.</p> <p>Note: The EdgeSight for Endpoints agent does not collect session-related data on XenDesktop systems. If you wish to collect data relating to XenDesktop, please install the EdgeSight for Virtual Desktop Agent.</p>
<p>NO_CONTROL_PANEL</p>	<p>Determines whether the control panel applet is installed.</p> <p>0=Install control panel applet.</p> <p>1=Do not install control panel applet.</p> <p>Default value is 0.</p> <p>For more information, see Configuring Agents Using the Control Panel.</p>
<p>FUNCTIONALITY_MODE</p>	<p>The operational mode (Basic or Advanced) for an EdgeSight for XenApp agent, as described in “Agent Mode” in Installing EdgeSight Agents. The option values as are follows:</p> <p>1 = Advanced Mode</p> <p>2 = Basic Mode</p>

SHOW_SERVICES_TAB	<p>Determines whether the Service Control tab is displayed on the control panel applet. The tab allows users to enable or disable the Citrix System Monitoring Services.</p> <p>0 = Services tab not displayed.</p> <p>1 = Services tab displayed.</p> <p>Default values are disabled (0) for EdgeSight for Endpoints Agents and enabled (1) for EdgeSight for XenApp Agents.</p> <p>See Configuring Agents Using the Control Panel for more information on the control panel applet.</p>
OVERRIDE_COMPCHECK	<p>Overrides the version check described in “Antivirus Configuration Checking” in Installing EdgeSight Agents. To override the check, specify this property with a value of 1.</p> <p>Note: This property should only be used if you disable the McAfee buffer overflow protection feature as described under "Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent" in the Known Issues topic for your release.</p>
Network Settings	
CONNECTION_FLAGS	<p>0 = No SSL</p> <p>1 = Use SSL</p> <p>Default value is 0.</p>
HTTP_TIMEOUT	<p>Determines how long to wait, in seconds, for a connection or other operation to complete. The default value is 30 seconds.</p>
PROXY_FLAGS	<p>0 - No proxy settings are selected</p> <p>1 - Use proxy</p> <p>3 - Use proxy and non-SSL tunnel (CONNECTION_FLAGS must be set to 0)</p> <p>5 - Use proxy and require authentication (value must be supplied for PROXY_USER)</p> <p>7 - Use proxy and require authentication (value must be supplied for PROXY_USER) and non-SSL tunnel (CONNECTION_FLAGS must be set to 0)</p> <p>Default value is 0.</p>
PROXY_PORT	<p>Port through which the agent communicates with the proxy server. The default port number is 8080.</p>

PROXY_ADDRESS	The hostname or IP address for the proxy server.
PROXY_USER	The user name for the account used to access the proxy server.
PROXY_PASSWORD	Password for access to the proxy server. The password is encrypted before being stored in the registry.
SERVER_NAME	Server to which the agent will report data. This property is required. If no server name is supplied, the agent is unable to upload data to the server.
SERVER_PORT	Port through which the agent communicates with the EdgeSight Server. The default port number is 80.
FIREWALL_EXCEPTION_ALLOWED	Supply a value of 1 to allow Windows Firewall to be automatically configured to exclude the listen port (9035). The firewall must be running, but can either be enabled or disabled. If you do not want the firewall automatically configured, set the value to 0. The default value is 1.
Virtual Desktop Environment Properties	These properties are only used when installing the EdgeSight for Endpoints Agent on virtual desktops in a pool. See Installing EdgeSight for Monitoring Virtual Desktops for more information.
POOLED_INSTALL	Supply a value of 1 to indicate that the agent is to be installed on virtual desktops in a pool. This property must be set to 1 to enable the remaining virtual desktop environment properties.
REMOTE_PATH	The UNC path for the agent data file share.
IMAGE_POOL	The name of the pool in which the virtual desktops will be running. This pool name is case sensitive and must match the pool name specified during the agent database server installation.
DBBROKER_FQDN	The fully-qualified domain name or IP address of the EdgeSight Server which will be acting as the database broker.
BROKER_PORT	The port associated with the EdgeSight Server which will be acting as the database broker.
BROKER_CONNECTION_FLAGS	0 = No SSL 1 = Use SSL
BROKER_PROXY_FLAGS	0 = No proxy 1 = Proxy is of CERN type 2 = Proxy is a non-SSL tunnel to an SSL server
BROKER_PROXY_ADDRESS	The hostname or IP address of the proxy server.
BROKER_PROXY_PORT	Port through which the agent communicates with the proxy server.
BROKER_PROXY_USER	The username used when accessing the proxy server.

BROKER_PROXY_PASSWORD	Password for access to the proxy server. The password is encrypted before being stored in the registry.
-----------------------	---

Use the `msiexec` command to install the agent using the command-line interface. Public properties are specified as *KEY=value* pairs as described earlier in this topic. If a property has a default value, that value is used if the property is not specified on the command line. When performing an installation using the command line, the following properties should always be specified:

- **SERVER_NAME**—If the server name is not specified, the agent is unable to obtain configuration information or upload data.
- **COMPANY**—If the company name is not specified, the device is considered an unmanaged device and cannot upload data to the server.

ALLOWSERVEROS should be specified if you attempt to install an EdgeSight for Endpoints agent on a system running a server OS. If this property is not specified, a warning is issued. During a silent installation to a system running a server OS, the install fails unless the **ALLOWSERVEROS** property is set to 1.

ALLOWVIRTUAL should be specified if you attempt to install an EdgeSight for Endpoints agent on a virtual desktop instance running XenDesktop 4.0. If this property is not specified, a warning is issued. During a silent installation to a virtual desktop instance running XenDesktop 4.0, the install fails unless the **ALLOWVIRTUAL** property is set to 1.

The following is a sample command line for the installation of an EdgeSight for Endpoints agent on a 64-bit desktop system:

```
Msiexec /i EdgeSightEPAgentx64.msi /l logfile.log /q  
SERVER_NAME=Myserver COMPANY=Mycompany DEPARTMENT=Mydept
```

The following is a sample command line for the installation of an EdgeSight for XenApp Agent on a 32-bit system running a server OS:

```
Msiexec /i EdgeSightXAAgent.msi /l logfile.log /q  
SERVER_NAME=Myserver COMPANY=Mycompany DEPARTMENT=Mydept  
ALLOWSERVEROS=1 DATA_DIR="d:\Mydata"
```

The `/i` flag is used to specify the package being installed. The `/l` flag is used to specify the installation log file name. (Capturing an installation log is strongly recommended.) Use the `/q` (quiet) flag to install an agent with no user interaction. For a complete list of standard MSI command-line arguments, open a Command Prompt window and type `msiexec /h` to invoke help, or refer to The Command-Line Options for the Microsoft Windows Installer Tool `Msiexec.exe` at <http://support.microsoft.com/kb/314881>.

Installing the EdgeSight for XenApp Agent in a Streamed Environment

Using the EdgeSight for XenApp Agent, you can implement monitoring of XenApp servers running in a streamed environment using Citrix Provisioning Server for Datacenters 4.5.

The Provisioning Server solution's streaming infrastructure is based on software streaming technology. It allows administrators to create a virtual disk (vDisk) that represents a computer hard drive, and then relocate that vDisk on an OS-Provisioning Server, or on a storage device that has access to a Provisioning Server. Once the vDisk is available, the target device no longer needs its local hard drive to operate; it boots directly across the network. The Provisioning Server streams the contents of the vDisk to the target device on demand, in real time, and the target device behaves as if it is running from its local drive.

Important: Although the operating system and applications are streamed to the target device, the EdgeSight Agent requires a persistent local drive to store its database.

Please review the following installation and configuration guidelines before deploying the EdgeSight for XenApp Agent in this environment.

Prerequisites

EdgeSight Server, Provisioning Server 4.5 for Datacenters, and the Citrix License Server for Windows must be installed on their respective machines. For installation instructions, refer to the following product documents:

- [Installing EdgeSight Server](#)
- [Citrix Provisioning Server 4.5 Installation and Administration Guide](#)
- "Getting Started with Citrix Licensing" under [Licensing Your Product](#)

Installing the EdgeSight Agent on a Master Target Device

After installing the Provisioning Server Target Device software on the master target device, but prior to imaging the system, install the EdgeSight agent. You can install the agent using the command-line or the user interface. In either case, keep in mind the following:

- All target devices associated with a virtual disk (vDisk) must report to the same EdgeSight Server. If a subset of machines is to report to a different EdgeSight Server, create a new vDisk for these devices.

- EdgeSight Agents detect when the vDisk is in private mode and will not start. This capability eliminates the need to set the EdgeSight agent service start mode to manual.
- If the master target device has only one disk drive, the installer will not allow a nonexistent drive to be specified. Registry and file system changes are required before master target imaging. See “Installation on a Master Target Device with a Single Disk” in [Installing the EdgeSight for XenApp Agent in a Streamed Environment](#) for more information.

Installing the Agent Using the Command-Line Interface

The SERVER_NAME and COMPANY parameters should always be specified to ensure that configuration information can be obtained from the server and that data can be uploaded to the server. The following sample command line also shows the use of the DATA_DIR parameter to select the data files folder. Note that the data directory cannot be on a mapped drive.

```
miexec.exe /i EdgeSightXAAgent.msi /l logfile.log /q  
SERVER_NAME=rsbetx COMPANY=Mycompany DATA_DIR="d:\Citrix\System  
Monitoring\Mydata"
```

Installing the Agent Using the User Interface

In the Agent Location dialog, be sure to install the EdgeSight agent on the virtual disk (vDisk). The default location can be used. Change the data folder to a location on the physical disk that will be in each target device. Note that the data directory cannot be on a mapped drive.

In the Network Settings dialog, specify the server name and port number for the EdgeSight Server. All target devices that use the vDisk will report to this server. If a subset of target devices is going to report to a different EdgeSight server, a separate vDisk must be created for those devices. (Do not change the network settings on an individual device; these changes are not persisted if the device is rebooted.)

Installation on a Master Target Device with a Single Disk

If the master target device has only one disk drive, the installer will not allow you to specify a data folder on a nonexistent drive. In this case, perform the installation using the default values and then edit the registry and file system when the installation completes:

1. Within the registry, navigate to the key `HKLM\Software\Citrix\System Monitoring\Agent\Core\4.00` and change the DataPath to the appropriate location

on the physical disk of the target devices.

2. Within the file system, navigate to %ProgramFiles%\Citrix\System Monitoring\Agent\Core\Firebird and locate aliases.conf.
3. Open aliases.conf in a text editor and change the `RSData` entry to match the location of the data folder on the physical disk of the target devices. For example: `RSData = D:\Citrix\System Monitoring\Data\RSData.fdb`

Imaging the Master Target Device Disk

Image the disk of the master target device.

Configuring Target Devices

Each target device must have a physical disk drive. The drive must have an NTFS partition that is visible to the streamed OS.

Set the boot order of the target device to boot from the network first.

Boot the target device from the shared vDisk. After booting the target device, the Citrix System Monitoring Agent service should be running and the service's data should be present on the target device's disk drive. If you need to troubleshoot a specific target device, registry changes for additional tracing should be made on the device, not on the vDisk. Note that these changes are not persisted if the device is rebooted.

Configuring Agents Using the Control Panel

If you need to reconfigure connection settings for agent to server communication after installation, use the Citrix System Monitoring Agent control panel applet. You must have Administrator privileges on the machine to launch the applet. To use the applet:

1. From the **Start** menu, choose **Settings > Control Panel** and select **Citrix System Monitoring Agent** to display the Citrix System Monitoring Agent Settings dialog.
2. Edit the Citrix EdgeSight Server address and port number as required.
3. Select the **Use SSL encryption** checkbox if the Citrix EdgeSight Server is SSL enabled. To be SSL enabled, a valid SSL certificate issued by a trusted certificate authority must be present on the server running the Citrix EdgeSight Web site. If SSL support is enabled, all agent to server communications must be over SSL. If an agent attempts to connect to an SSL-enabled server without using SSL, an error is generated and the data upload is rejected.
4. Select the **Use a proxy server** checkbox if a proxy server is used. Enter the proxy server address and port and indicate whether the server is a non-SSL tunnel and whether authentication is required. Supply the authentication username and password if required.
5. If an EdgeSight for XenApp agent is installed on a machine running XenApp Enterprise, you can select the **Mode** tab and change the agent mode (Basic or Advanced). Note that this tab is not displayed on XenApp Platinum systems. For more information on agent modes, see “Agent Mode” in [Installing EdgeSight Agents](#).
6. When you have made all required settings changes, click **OK** to apply the changes and close the dialog. If the Service Control tab has been enabled on the control panel applet, you can disable or enable the Citrix System Monitoring Service and the Firebird Server - CSMinstance service. Disabling these services stops the services and sets the startup type to disabled. Enabling the services starts the services and sets the startup type to automatic.

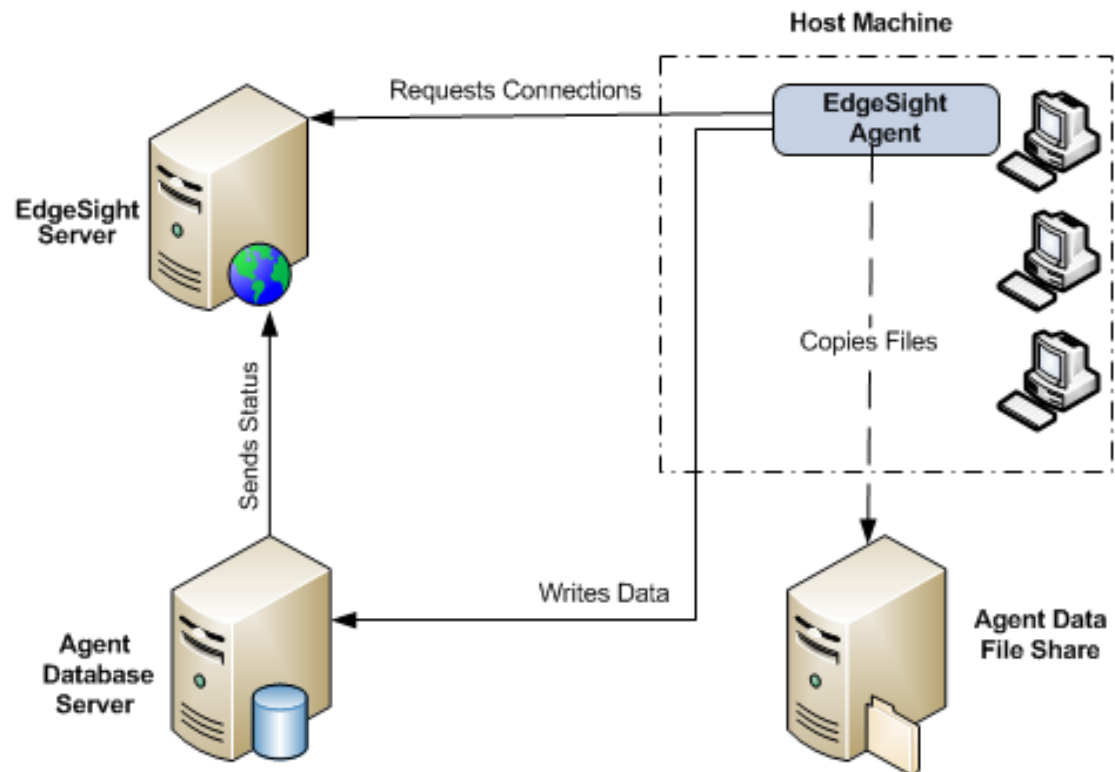
Important: The Service Control capability is intended for use in the event that you suspect that an EdgeSight Agent is causing performance or software compatibility problems. By using the Service Control feature, you can disable services and keep them from restarting. If you uninstall the agent when a problem occurs, you may lose data which may help in resolving the problem.

The Service Control tab is enabled by default for EdgeSight for XenApp agents, but it is disabled by default for EdgeSight for Endpoints agents.

The Service Control tab can be displayed by setting the SHOW_SERVICES_TAB parameter to 1 during agent installation, or by setting the
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\System
Monitoring\Agent\Core\4.00\Control Panel\AllowServiceControl registry
key to 1.

Installing EdgeSight for Monitoring Virtual Desktops

When monitoring physical endpoint machines, EdgeSight Agents store performance and availability data in a local database. Because virtual desktops in a pool are not preserved across reboots, agents must store data externally on a database server and a file share. The following figure shows the components required for virtual desktop monitoring.



- EdgeSight Server—In addition to displaying reports and providing an interface for administration and configuration, EdgeSight Server includes database broker components which respond to agent requests for a connection string to an EdgeSight Agent Database Server.
- EdgeSight Agent Database Server—The EdgeSight Agent Database Server provides storage for data collected by EdgeSight Agents running on virtual desktops in a pool. During installation you will be asked to specify the name of the pool and the name of the EdgeSight Server which will act as the database broker. (Multiple agent database servers can be associated with a pool.) Once the agent database server has been installed, it registers with the EdgeSight Server and regularly reports its operational status.

- **Agent Data File Share**—The agent data file share provides storage for files such as log files and INI files which are not stored on the EdgeSight Agent Database Server. It is recommended that you set up your file share on either the EdgeSight Server or on an agent database server machine.
 - **EdgeSight for Virtual Desktops Agent or EdgeSight for Endpoints Agent**—The agent you install depends on the virtual desktops being monitored. If you are monitoring virtual desktops running XenDesktop 4.0, use the EdgeSight for Virtual Desktops Agent. If you are monitoring virtual desktops running XenDesktop 3.0, use the EdgeSight for Endpoints Agent. Initially, the EdgeSight Agent requests a connection string to an EdgeSight Agent Database Server. Once the agent is operational, it writes data to the agent database server and copies files to the agent data file share.
1. Install the EdgeSight Server that will also act as the broker for remote agent databases. See [Installing EdgeSight Server](#) for details.
 2. Install one or more agent database servers for each pool. See [Installing the Agent Database Server](#) for details.
 3. Setup a file share for agent data that does not reside in the database. See [Setting Up the Agent Data File Share](#) for details.
 4. Install the EdgeSight Agent on the disk to be used by virtual desktops. See [Installing the Agent](#) for details. For overall system requirements for a virtual desktop environment, see “Virtual Desktop Monitoring Requirements” in [System Requirements](#).

Installing EdgeSight Server

EdgeSight Server software includes components that assist agents running on virtual desktops to locate and connect to remote databases. When you install the EdgeSight Server Website, it additionally installs Web services that perform the following operations:

- Broker database connections for agents running on virtual desktops in a pool
- Monitor the status of available agent databases

These components are installed by default; you do not have to explicitly select or configure them. This allows you to easily designate a different EdgeSight Server as the database broker.

If you have multiple EdgeSight Server installations, you need only select one to act as the database broker, though you may designate others if you wish. The EdgeSight Server that will act as the database broker is selected when you install the agent database server, as described in [Installing the Agent Database Server](#). Note that if an EdgeSight Server is not brokering database connections, no status information will be displayed on the Agent Database Broker pages of the server console. See [Installing EdgeSight Server](#) for detailed instructions on installing EdgeSight Server software.

Installing the Agent Database Server

The agent database server can be installed on a Windows physical or virtual server-class machine. The installation creates a database monitor. An agent database is created when an agent is brokered to the agent database server. The database stores data written by an EdgeSight Agent, while the database monitor reports database availability and status to the EdgeSight Server acting as a database broker. If a firewall is installed on the machine, port 9037 must be open to allow communication with EdgeSight agents. Each agent database server can support one image pool.

During installation you will be asked to specify the name of the pool and the name of the EdgeSight Server which will act as the database broker. Typical disk space usage is generally 70 MB per virtual desktop for the databases on a single disk. After the installation is complete, the database monitor reports the availability of the agent database server to the database broker.

1. Insert the media.
2. Select **EdgeSight Component Installers**.
3. Select **EdgeSight Agent Database Server** to display the installer Welcome page.
4. Click **Next** to display the End User License Agreement page.
5. After reading the license agreement, select the **I accept** radio button and click **Next** to display the Network Settings page.
6. Enter the broker name and port. The broker name is the name of the machine hosting the previously installed EdgeSight Server, which includes the database broker components. You can also enter an IP address or fully qualified domain name.
7. The **Automatically configure Windows Firewall for Port 9037** checkbox is selected by default. Enabling this feature automatically configures the firewall for the database listen port (the port on which the agent database server listens for remote connections from the database broker). The firewall must be running, but can either be enabled or disabled. The exclusion is set up for Domain networks. If an exception for Private networks is required, the Domain exception can be used as a template. If you do not want Windows Firewall automatically configured, deselect the checkbox.
8. If an SSL network connection is required, select the **Use SSL** checkbox.
9. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server.
10. After specifying the network settings, click **Next** to display the Agent Location screen.
11. Enter the installation path for the agent database server or accept the default value. You can browse to select a non-default location.
12. Enter the installation path for the data files or accept the default. You can browse to select a non-default location.

13. Enter a name for the pool hosting the agents which will store data on the agent database server. You can choose any pool name. For ease of use, you may want to choose one that corresponds to the XenDesktop desktop group name.
14. Click **Next** to display the Ready to Install screen.
15. Click **Next** to begin the installation and display the Performing Installation screen. When the installation is complete, the Setup Complete page is displayed.
16. Click **Finish** to exit the setup wizard.

Setting Up the Agent Data File Share

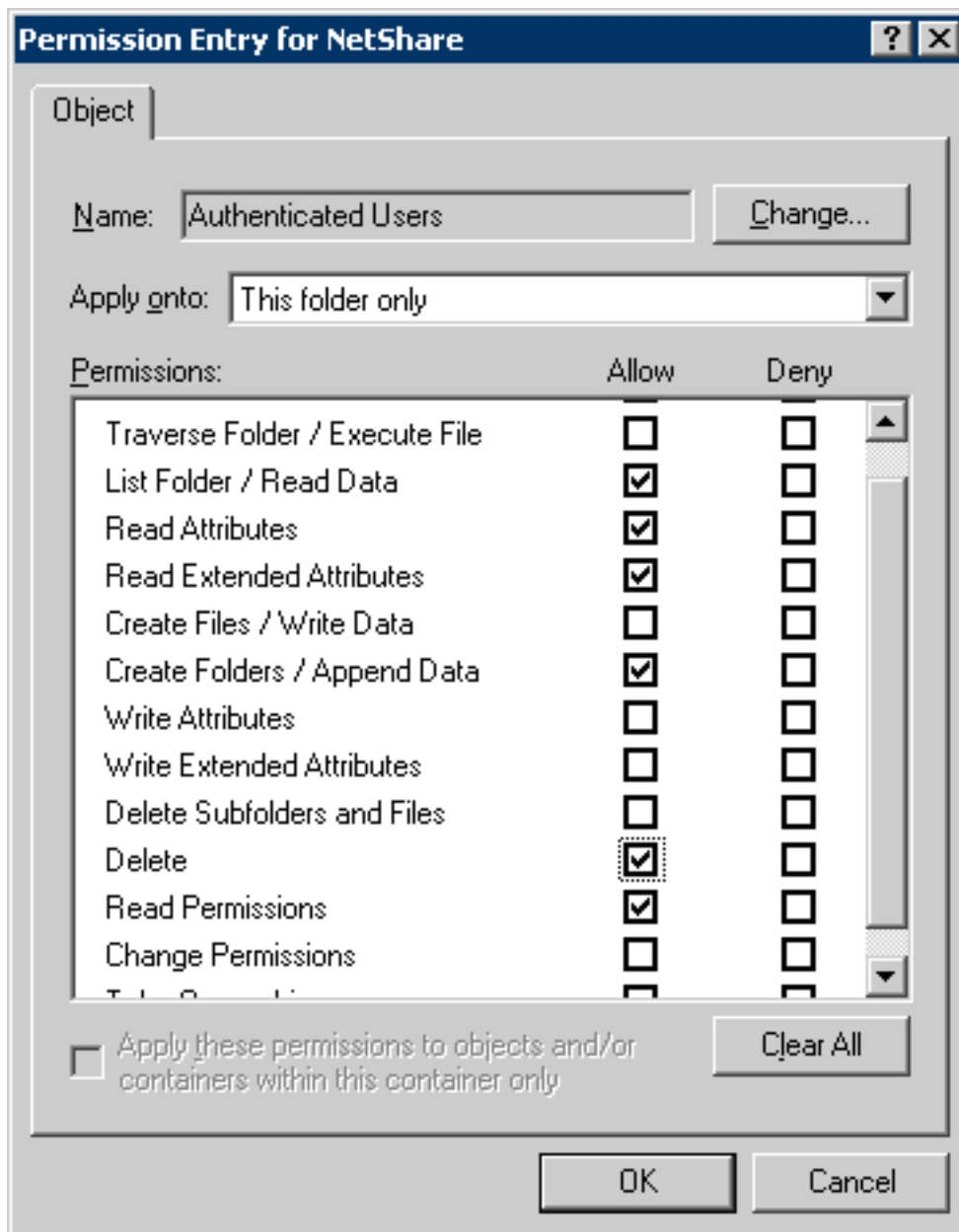
Some agent data are not stored in the agent database, such as log files and INI files. Therefore, agents running on virtual desktops require access to an external file share. The file share must be configured with permissions allowing authenticated users to create subdirectories that will contain the files, plus settings. The disk space needed is minimal and the file copies are small and infrequent. It is recommended that you set up your file share on either the EdgeSight Server or on an agent database server machine.

On Windows 2003 Systems

The permissions required include both the file share permissions and the NTFS file system permissions. To create an agent data file share and set all permissions on a Windows 2003 system:

1. Create a new folder. The file share should not be located on a specific user's desktop. Record the folder UNC path for use during the agent installation process.
2. Right click on the folder name and select **Properties** from the popup menu to display the Properties dialog.
3. Select the **Sharing** tab. Select the **Share this folder** radio button.
4. Click the **Permissions** button to display the Permissions dialog.
5. Click **Add** to display the Select Computer, User, or Group dialog.
6. Enter **Authenticated Users** in the **Enter object name to select** field. Click **OK**.
7. Select the **Authenticated Users** group.
8. Ensure that the **Change** and **Read** permissions are selected and click **OK**.
9. Select the **Security** tab and click the **Advanced** button to display the Advanced Security Settings dialog.
10. Deselect the checkbox which enables child objects to inherit permission entries from the parent. (The specific checkbox label may vary based on the operating system.) When this setting is disabled, a Security dialog is displayed advising you that permission entries will no longer be inherited. Click **Remove**.
11. Click **Add** to display the Select Computer, User, or Group dialog.
12. Enter **Authenticated Users** in the **Enter object name to select** field. Click **OK** to display the Permission Entry dialog.
13. Select **This folder only** from the **Apply onto** drop down menu.
14. Ensure that the following permissions are allowed:

- List Folder / Read Data
- Read Attributes
- Read Extended Attributes
- Create Folders / Append Data
- Delete
- Read Permissions



15. Click **OK** on all open dialog boxes.

On Windows 2008 Systems

To create an agent data file share and set all permissions on a Windows 2008 system:

1. Create a new folder. The file share should not be located on a specific user's desktop. Record the folder UNC path for use during the agent installation process.
2. Right click on the folder name and select **Properties** from the popup menu to display the Properties dialog.
3. Select the **Sharing** tab. Select the **Share** button to display the File Sharing dialog.
4. Enter **Authenticated Users** in the text entry field. Click **Add**.
5. Select the **Authenticated Users** group and click on **Contributor** in the drop-down menu.
6. Click **Share**. When the operation is complete, click **Done**.
7. Select the **Security** tab, select **Authenticated Users** from the list of groups and user names. Click the **Advanced** button to display the Advanced Security Settings dialog.
8. Select **Authenticated Users** from the list of permission entries and click **Edit** to display the Advanced Security Settings dialog.
9. Deselect the checkbox which enables child objects to inherit permission entries from the parent. (The specific checkbox label may vary based on the operating system.) When this setting is disabled, a Security dialog is displayed advising you that permission entries will no longer be inherited. Click **Remove**.
10. Select **Authenticated Users** from the list of permission entries and click **Edit** to display the Permission Entry dialog.
11. Select **This folder only** from the **Apply to** drop down menu.
12. Ensure that the following permissions are allowed:
 - List Folder / Read Data
 - Read Attributes
 - Read Extended Attributes
 - Create Folders / Append Data
 - Delete
 - Read Permissions
13. Click **OK** on all open dialog boxes.

Prerequisites for Installing EdgeSight Agents

Before installing the agent in a virtual desktop environment, you must perform the following tasks:

1. Ensure that you have the information required during agent installation.
2. Place the group of virtual desktops in maintenance mode and then shut them down.
3. Set the vDisk access mode to private.

Note: This procedure assumes that you are working with an existing master image. You can also install the agent as part of creating a master image prior to sharing the image out to the pool.

Shutting Down Virtual Desktops

Important: Before shutting down virtual desktops, ensure that they are not in use to avoid loss of data.

Before installing the agent in a virtual desktop environment, you must ensure that the virtual desktops are in maintenance mode and are then shut down. To set the virtual desktops to maintenance mode and shut them down:

1. Log on to the Desktop Delivery Controller (DDC) for the target desktop group and open the Citrix Access Management Console.
2. Navigate to **Citrix Resources > Desktop Delivery Controller > FarmName > Desktop Groups** and click on the target group to display a list of the virtual desktops.
3. Select all desktops in the group and right click on the group to display the pop-up menu. Select **Enable maintenance mode** to temporarily stop connections to the desktops.
4. Right click on the group again and select **Shutdown/suspend** from the pop-up menu to display the Shutdown/suspend dialog.
5. Select **Shut down** from the drop-down menu and click **OK**. (You may need to refresh the display to update the status displayed for the desktops.)

Setting the vDisk Access Mode to Private

You must set the access mode property for the vDisk associated with the target desktop group.

1. Log on to the Provisioning Server associated with the vDisk on which the EdgeSight Agent will be installed and start the Provisioning Server Console.
2. Navigate to **FarmName** > **Stores** and select the store associated with the target vDisk.
3. Right click on the vDisk and select **Properties** from the pop-up menu.
4. Click on the **Edit file properties** button to display the vdisk File Properties dialog.
5. Select the **Mode** tab.
6. Select **Private access (single device, R/W access)** from the **Access Mode** drop down menu and click **OK**.
7. Click **OK** in the vdisk File Properties dialog.

Information Required During Agent Installation

Ensure that you have the following information at hand before installing the agent software on the master image:

- The UNC path name of the agent data file share. The Network Service that will be running on desktops will need to be able to create directories and copy files to this share.
- The fully-qualified domain name or IP address of the EdgeSight Server that will be acting as the database broker. In addition to the server name you can specify the port and SSL or proxy server information, if used.
- The name of the pool in which the virtual desktops will be running. This pool name is case sensitive and must match the pool name specified during the agent database server installation. The pool name corresponds to the XenDesktop desktop group name.

Installing the Agent

You install the EdgeSight for Virtual Desktops Agent or the EdgeSight for Endpoints Agent on the master image. During the installation, you indicate that the agent is being installed on virtual desktops. After the agent installation is complete, you must reboot your master image.

Software Configuration Tasks

You may need to change the configuration of some software, such as antivirus software or personal firewalls, on machines which will run the EdgeSight Agent and will host the agent database server and the agent data file share to ensure proper operation. You can perform these configuration tasks before or after installing the EdgeSight Agent. For more information, see [Configuring Third Party Software](#).

If you are running a firewall on the machine hosting the agent database server, the port used to communicate with EdgeSight agents must be open. The default port is 9037.

Antivirus Configuration Checking

Due to the manner in which buffer overflow protection was implemented in McAfee VirusScan 8 or 8i with Patch 10, this feature which may conflict with the operation of the EdgeSight Agent. (In later versions of McAfee VirusScan, this feature was implemented differently and does not conflict with EdgeSight Agent operation.) The EdgeSight Agent installer checks for McAfee 8 or 8i with Patch 10 or below on the target machine. If the EntApi.dll file is present with version 8.0.0.277 and below, the installation exits with an error. The check is performed on both full UI and unattended installations. In a command-line installation, the check can be omitted from the installation process by specifying the `OVERRIDE_COMPCHECK` property with a value of 1.

Note: The `OVERRIDE_COMPCHECK` property should only be used if you disable the McAfee buffer overflow protection feature as described under "Incompatibility Between McAfee Host Intrusion Protection (HIPS) V7.0 and the EdgeSight Agent" in the [Known Issues in EdgeSight 5.3](#).

Agent Installation Methods

The MSI file uses public properties to specify custom install settings. You can set public properties using the following methods:

- Run the installer user interface (if the property is exposed). This method offers fewer installation options than using the command-line interface. Also, a log file is not created when the user interface is used for installation.
- Create a transform file using a tool such as Orca.

- Specify key/value pairs on the command line. This method allows you to control the full range of installation options, including specifying a log file, as well as being able to specify public properties. The syntax for key/value pairs is *KEY=value*.

See your MSI documentation for syntax rules for property values. See [Installing EdgeSight Agents Using the Command Line](#) for definitions of the public properties used when installing the EdgeSight agent.

Installing an Agent Using the User Interface

Note that not all public properties listed in [Installing EdgeSight Agents Using the Command Line](#) are exposed when installing using the user interface. Properties not explicitly set from the user interface are set to their default value if one exists. To install an agent using the user interface:

1. Insert the media.
2. Select **EdgeSight Agent Installers**.
3. Select **EdgeSight for Virtual Desktops Agent** or **EdgeSight for Endpoints Agent** to display the Welcome screen.
4. Click **Next** to display the License Agreement screen.
5. After reading the license, select the **I accept** radio button and click **Next** to display the Company Information screen.
6. Enter the company name. If you are installing an EdgeSight for Endpoints agent for monitoring XenDesktop 3.0 instances, you can also specify a department. If no department name is provided, the agent data will be displayed under the root department. If you are installing an EdgeSight for Virtual Desktops agent for monitoring XenDesktop 4.0 instances, the department field cannot be set because the department is determined by the XenDesktop Farm structure. Click **Next** to display the Agent Location screen.
7. Enter the installation path for the agent or accept the default value. You can browse to select a non-default location.
8. Enter the installation path for the data files or accept the default. You can browse to select a non-default location. Click **Next** to display the Network Settings screen.
9. Enter the server name and port number. These are required fields.
10. If an SSL network connection is required, select the **Use SSL** checkbox. (This is equivalent to setting the CONNECTION_FLAGS property.)
11. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server. (This is equivalent to setting the PROXY_ADDRESS, PROXY_PORT, and PASSWORD properties.) Click **Next** to display the Advanced Settings screen.
12. Select the **Configure the agent for virtual desktops** checkbox.

13. In the **Remote UNC Path** field, enter the UNC path for the agent data file share, for example `\\Myserver.mydomain.com\AgentFiles`. For information on setting up the file share, see [Setting Up the Agent Data File Share](#).
14. In the **Pool Name** field, enter the name of the pool in which the virtual desktops will be running. This pool name is case sensitive and must match the pool name specified during the agent database server installation, as described in [Installing the Agent Database Server](#).
15. In the **Database Broker** field, enter the fully-qualified domain name of the EdgeSight Server which will be acting as the database broker. (The database broker components are installed on every EdgeSight Server and cannot be installed separately or moved.)
16. If an SSL network connection is required, select the **Use SSL** checkbox.
17. If a proxy server is used, select the **Use a proxy server** checkbox. Then enter the proxy server name and port and the username/password used to access the server. Click **Next** to display the Ready to Install screen.
18. If you need to review or change any settings before installing, use the **Back** button to return to the configuration screens.
19. Click **Install** to begin the installation. When the installation is complete, the Setup Complete screen is displayed.
20. Click **Finish** to complete the installation. The Installer Information dialog prompts you to reboot your system so that configuration changes will be applied.
21. Click **Yes** to reboot your machine. It is recommended that you flush the DNS cache after rebooting the machine (`ipconfig /flushdns`). This can help prevent errors related to DNS caching when the agent initially accesses the network.

Installing an Agent Using the Command-Line Interface

Use the `msiexec` command to install the agent using the command-line interface. Public properties are specified as `KEY=value` pairs as described in [Installing EdgeSight Agents Using the Command Line](#). If a property has a default value, that value is used if the property is not specified on the command line. When performing an installation in a virtual desktop environment using the command line, the following properties should always be specified:

- `SERVER_NAME`—If the server name is not specified, the agent is unable to obtain configuration information or upload data.
- `COMPANY`—If the company name is not specified, the device is considered an unmanaged device and cannot upload data to the server.
- `POOLED_INSTALL`—This flag and the following properties are required so that the agent can communicate with the database broker components of EdgeSight Server and can copy and retrieve files from the agent data file share.
- `REMOTE_PATH`
- `IMAGE_POOL`

- `DBBROKER_FQDN`
- `BROKER_PORT`

`ALLOWSERVEROS` should be specified if you attempt to install a Citrix EdgeSight for Endpoints agent on a system running a server OS. If this property is not specified, a warning is issued. During a silent installation to a system running a server OS, the install fails unless the `ALLOWSERVEROS` property is set to 1.

`ALLOWVIRTUAL` should be specified if you attempt to install an EdgeSight for Endpoints agent on a virtual desktop instance running XenDesktop 4.0. If this property is not specified, a warning is issued. During a silent installation to a virtual desktop instance running XenDesktop 4.0, the install fails unless the `ALLOWVIRTUAL` property is set to 1.

The following is a sample command line for the installation of an EdgeSight for Endpoints agent on a 64-bit virtual desktop system:

```
Msiexec /i EdgeSightEPAgentx64.msi /l logfile.log /q  
SERVER_NAME=Myserver COMPANY=Mycompany DEPARTMENT=Mydept  
POOLED_INSTALL=1 REMOTE_PATH="\\Myserver.mydoain.com\AgentFiles"  
IMAGE_POOL=Pool2 DBBROKER_FQDN=Myserver.dom1.com BROKER_PORT=80
```

The `/i` flag is used to specify the package being installed. The `/l` flag is used to specify the installation log file name. (Capturing an installation log is strongly recommended.) Use the `/q` (quiet) flag to install an agent with no user interaction. For a complete list of standard MSI command-line arguments, open a Command Prompt window and type `msiexec /h` to invoke help, or refer to The Command-Line Options for the Microsoft Windows Installer Tool Msiexec.exe at <http://support.microsoft.com/kb/314881>.

Deploying the Agent to Virtual Desktops in a Pool

To deploy the agent to the virtual desktops in a pool, perform the following tasks:

1. Shut down the master image.
2. Set the access mode property for the vDisk associated with the target desktop group to **Standard Image**.
3. Disable maintenance mode on the desktop group.

Note: This procedure assumes that you are working with an existing master image. You can also install the agent as part of creating a master image prior to sharing the image out to the pool. If you are not working with an existing vDisk, create the vDisk at this point in the procedure.

Shutting Down the Master image

The master image must be shut down so that the access mode property for the vDisk can be changed.

Setting the vDisk Access Mode

You must set the access mode property for the vDisk associated with the target desktop group.

1. Log on to the Provisioning Server associated with the master image on which the EdgeSight Agent was installed and start the Provisioning Server Console.
2. Navigate to **FarmName** > **Stores** and select the store associated with the target vDisk.
3. Right click on the vDisk and select **Properties** from the pop-up menu.
4. Click on the **Edit file properties** button to display the vdisk File Properties dialog.
5. Select the **Mode** tab.
6. Select **Standard Image (multi-device, write-cache enabled)** from the **Access Mode** drop down menu and click **OK**.
7. Click **OK** in the vdisk File Properties dialog.

Disabling Maintenance Mode

To enable normal operation by the virtual desktops, you must ensure that maintenance mode is disabled. To disable maintenance mode for the desktop group:

1. Log on to Desktop Delivery Controller (DDC) for the target desktop group and open the Citrix Access Management Console.
2. Navigate to **Citrix Resources > Desktop Delivery Controller > *FarmName* > Desktop Groups** and click on the target group. A list of the virtual desktops is displayed.
3. Select all desktops in the group and right click on the group to display the pop-up menu. Select **Disable maintenance mode**.

Post-Installation Configuration

You may need to change incorrect configuration settings using the agent's control panel application.

Agent Database Connection Acquisition

When you configure the agent for virtual desktops, file monitor components are installed which manage copying files to and retrieving files from the agent data file share. The agent is configured to contact the database broker to receive a database connection string. If it fails to get a database connection, it shuts down and writes error information to the local SYS_EVENT_TXT.TXT log. If the file monitor components are functioning properly, a copy of the log file will also be placed on the agent data file share. You can change incorrect configuration settings using the agent's control panel application. However, you must make those changes on the master image in order for them to be propagated to all desktops.

Configuring Agents Using the Control Panel

If you need to reconfigure connection settings for agent to server communication after installation, use the Citrix System Monitoring Agent control panel applet. You must have Administrator privileges on the machine to launch the applet.

In a virtual desktop environment, any changes to these settings must be made on the master image and then deployed to the pool.

The Service Control tab is disabled by default for EdgeSight for Virtual Desktops and EdgeSight for Endpoints agents. The Service Control tab can be displayed by setting the SHOW_SERVICES_TAB parameter to 1 during agent installation, or by setting the HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\System Monitoring\Agent\Core\4.00\Control Panel\AllowServiceControl registry key to 1.

To use the applet:

1. From the **Start** menu, choose **Settings > Control Panel** and select **Citrix System Monitoring Agent** to display the Citrix System Monitoring Agent Settings dialog.
2. Select the **Remote Share** tab. Edit the UNC path to the agent data file share as required.
3. Select the **EdgeSight Server** tab. Edit the Citrix EdgeSight Server address and port number as required.
4. Select the **Use SSL encryption** checkbox if the Citrix EdgeSight Server is SSL enabled. To be SSL enabled, a valid SSL certificate issued by a trusted certificate authority must be present on the server running the Citrix EdgeSight Web site. If SSL support is enabled, all agent to server communications must be over SSL. If an agent attempts to connect to an SSL-enabled server without using SSL, an error is generated and the data

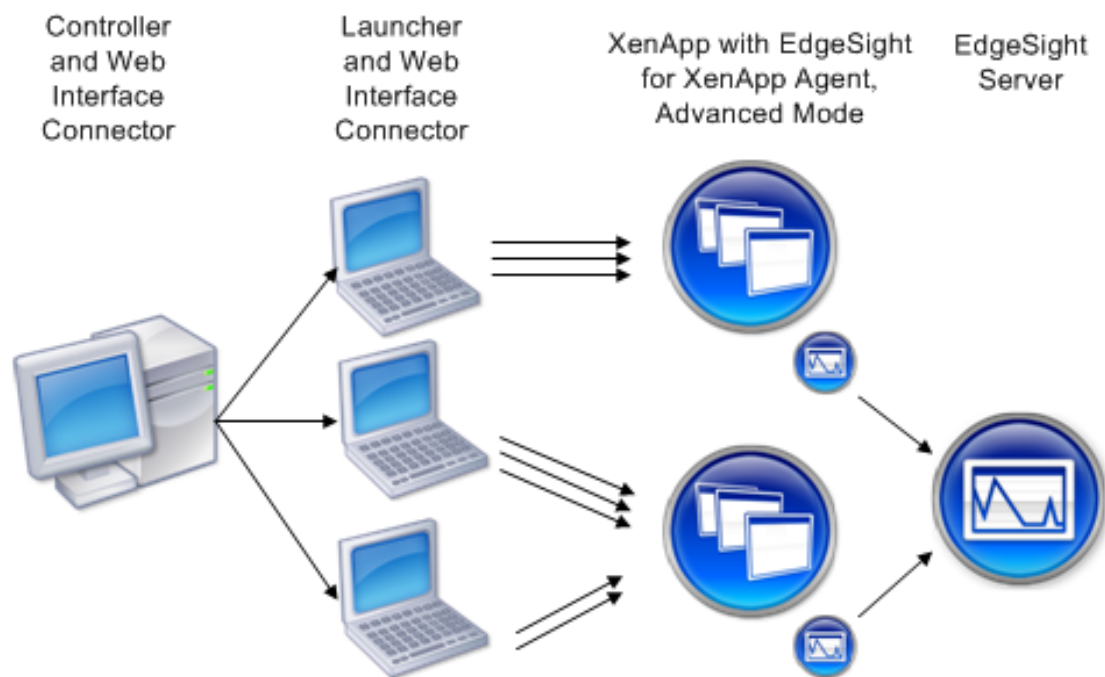
upload is rejected.

5. Select the **Use a proxy server** checkbox if a proxy server is used. Enter the proxy server address and port and indicate whether the server is a non-SSL tunnel and whether authentication is required. Supply the authentication username and password if required.
6. Select the **Broker Server** tab. Edit the address and port number for the EdgeSight Server acting as the database broker as required. You can also edit SSL and proxy server settings as described in steps 4 and 5.
7. When you have made all required settings changes, click **OK** to apply the changes and close the dialog.

Important: The Service Control capability is intended for use in the event that you suspect that an EdgeSight Agent is causing performance or software compatibility problems. By using the Service Control feature, you can disable services and keep them from restarting. If you uninstall the agent when a problem occurs, you may lose data which may help in resolving the problem.

Installing EdgeSight Active Application Monitoring Software

EdgeSight AAM depends on the deployment of several software components. For AAM component system requirements, see “Active Application Monitoring Requirements” in [System Requirements](#).



1. Install EdgeSight Server, adhering to the system requirements listed in “Server Requirements” in [System Requirements](#).
2. Install the AAM Controller and Launcher, adhering to the system requirements listed in “Active Application Monitoring Requirements” in [System Requirements](#). These components can be installed on the same machine or on different machines.
3. Optionally, install the Web Interface Connector. This component is required if users will be connecting to XenApp systems using the XML service. The Web interface Connector requires the installation of Microsoft Visual J# .NET Redistributable Package.
4. Install the EdgeSight for XenApp Agent on each XenApp system to be tested, adhering to the system requirements listed in “Agent Requirements” in [System Requirements](#). The agent must be installed in Advanced Mode to ensure that AAM-related alerts can be generated.

The Launcher is installed as a service (Citrix EdgeSight Launcher Service). The default location for Launcher installation is:

%ProgramFiles%\Citrix\Citrix EdgeSight Simulation\LauncherService.exe

Launchers and the Controller use port 18747 to communicate.

After deploying the software components, you can perform the following tasks, as described in EdgeSight Active Application Monitoring Help and EdgeSight Server Online Help:

- Configure the systems to be tested, as well as the systems hosting the Controller and Launchers.
- Using the Controller, create a script, including monitoring points, and create virtual users.
- Using the EdgeSight Server Console, create Application Response Time and Application Response Failure alerts for real-time notification of application response times that exceed thresholds or application response failures.
- Using the EdgeSight Server Console, monitor applications under test using the Application Response Time and Application Response Failure historical reports.

Installing the Active Application Monitoring Components

Important: If you previously installed the AAM components included with the EdgeSight 5.3 release, you will be prompted to uninstall those components before running the EdgeSight AAM 5.3 Service Pack 1 installer.

Use the following steps to initially install the software:

1. Insert the media or run Autorun.
2. Select **EdgeSight Component Installers**.
3. Select **EdgeSight Active Application Monitoring Installation** to display the Welcome screen.
4. Click **Next** to display the License Agreement screen.
5. After reading the license, select **I accept** and click **Next** to display the Installation Type screen.
6. Select the type of installation you want to perform. If you selected Custom, go to Step 7. If you selected Typical or Complete, skip to Step 8.
 - Typical - Install the Controller and Launcher
 - Custom - Select the components you want to install from Controller, Launcher, and Web Interface Connector. When you use the Web Interface Connector, it must be installed on the Controller and Launcher. The Web Interface Connector allows users to connect to applications made available through the XML Service. This feature requires the Visual J# Version 2.0 Redistributable Package available from Microsoft at <http://msdn2.microsoft.com/en-us/vjsharp/default.aspx>.

- Complete - Install the Controller, Launcher, and Web Interface Connector.
7. By default, all components are enabled. To disable installation of a component, click the component and select **Entire feature will be unavailable**. Click **Disk Usage** to display disk space availability, or click **Reset** to return to the default component selections. When you have completed feature selection, click **Next**.
 8. The system prompts for a password. This password will be required when using each Launcher and the Controller. The password must be at least 8 characters in length and should match the passwords set on all Launcher machines to be used in the test.
 9. Click **Install** to install the software and display the Performing Installation Tasks screen. The Installation Complete screen is displayed after the software is installed.
 10. Click **Finish** to exit the Setup Wizard.
 11. After the installation is complete, go to **Citrix > Citrix EdgeSight Active Application Monitoring > AAM Controller** and log in using the previously specified password. Select **Help > Help Topics** to display online help. The help file includes information about configuring Controllers, Launchers, and XenApp systems under test.

Configuring Third Party Software

In some cases, you may need to perform software configuration tasks to ensure that EdgeSight works properly in your environment. Review the following guidelines and implement the recommendations as required. In addition, review the applicable release notes for release-specific configuration information.

Configuring Antivirus Software

You must configure antivirus software running on your EdgeSight Server and all managed devices (machines running EdgeSight Agent) to exclude specific processes and files. If these files and processes are not excluded, communications between the agents and the server may be disrupted, and performance on monitored devices can be degraded.

Note: The paths and filenames provided are based on default installation values for EdgeSight and other software components. If you have specified non-default paths and filenames, use the values applicable to your installation. You can use the About page on the EdgeSight Server Console to identify installation paths and filenames on the server.

To configure antivirus software on devices running EdgeSight Agent:

- Ensure that the following agent service, which is a script host, is not subject to script blocking:

`%ProgramFiles%\Citrix\System Monitoring\Agent\Core\rscorsvc.exe`

- Exclude the following folder. This folder contains the EdgeSight database, which is highly transactional, along with log files and temporary files:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\` for Microsoft Vista and Windows Server 2008 systems

`%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data\` for all other systems

If you have agents installed in a virtual desktop environment, exclude the following:

- The data folder on the EdgeSight Agent Database Server:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\` for Windows Server 2008 systems

`%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data\` for all other systems

- Agent data file share. See [Setting Up the Agent Data File Share](#) for more information on the file share configuration.

To configure antivirus software on your EdgeSight Server:

- Ensure that the following files, which are script hosts, are not subject to script blocking:

`%CommonProgramFiles%\Citrix\System Monitoring\Server\RSSH\ RSshApp.exe`

`%CommonProgramFiles%\Citrix\System Monitoring\Server\RSSH\ RSshSvc.exe`

- Exclude the following folder, which contains the Citrix EdgeSight Web server:

`%ProgramFiles%\Citrix\System Monitoring\Server`

- Exclude the SQL DB folder:

`%ProgramFiles%\Microsoft SQL Server\MSSQL\Data\`

- Exclude the IIS Web Site Log files:

`%SystemRoot%\SYSTEM32\Logfiles`

Configuring Firewalls

The listen port on the client machine (port 9035) must be open. This is the port on which the agent listens for remote connections from the browser displaying the Citrix EdgeSight console. There is an option during agent installation to automatically set a Windows Firewall exception for the listen port if the firewall is running (enabled or disabled).

If a firewall is installed on the machine hosting the EdgeSight Agent Database Server, port 9037 must be open to allow communication with EdgeSight Server. There is an option during agent database server installation to automatically set a Windows Firewall exception for the listen port if the firewall is running (enabled or disabled). The EdgeSight Agent Database Server is only installed when using the EdgeSight for Endpoints agent to monitor virtual desktops.

Certain types of ports must be opened to allow EdgeSight Server (specifically the User Troubleshooter) to communicate with XenApp. EdgeSight Server uses MFCOM to communicate with XenApp servers. MFCOM in turn uses DCOM and requires that RPC ports are opened on the XenApp server.

Upgrading EdgeSight

Upgrading or Uninstalling EdgeSight Server

Important: You should back up your EdgeSight database before performing an EdgeSight Server upgrade. Optionally, you may want to reboot your EdgeSight Server so that all EdgeSight processes are restarted, providing a known state from which to upgrade. Also, the EdgeSight Server should be upgraded before upgrading the associated EdgeSight agents.

You can directly upgrade to EdgeSight Server 5.3 from EdgeSight Server 5.0 SP2 and above.

The MSI file checks for existing versions of the Citrix EdgeSight database and Web server components each time you invoke server setup. Note that upgrades from Technology Preview releases are not supported.

The time it takes to perform an upgrade may be affected by the distribution of the database file group. Additional time may be required to perform file group moves during the upgrade. In addition, the size of the database will affect the time required to perform an upgrade.

If you are performing a database-only upgrade on a system hosting both the EdgeSight Web site and database, turn off IIS on the system before performing the upgrade. This will prevent EdgeSight from attempting to process data uploads and alerts at the same time that the database is being updated. In the case of a full update, IIS must be running to allow an IIS reset as part of the installation process.

Note: When you perform a server upgrade, support for EdgeSight for Virtual Desktops Agents (a new feature in EdgeSight 5.2), is not automatically enabled. If you will be monitoring XenDesktop 4.0 instances in your environment, perform the following steps to enable support for EdgeSight for Virtual Desktops Agents:

1. Open the EdgeSight Server Console.
2. Select the **Configuration** tab.
3. Navigate to **Server Configuration > Settings** and select the **Agent Support** tab.
4. Set **EdgeSight for XenDesktop Support** to **On**.

Upgrading or Uninstalling Agents

Important: Upgrading from a Technology Preview Release is not supported.

Important: Perform the EdgeSight Server upgrade before upgrading the associated EdgeSight agents.

There is no upgrade path associated with the EdgeSight for XenApp 6 Agent x64 5.3 (64-bit). This version of the agent is only supported for installation on XenApp 6.0 systems and requires a clean installation.

You can directly upgrade to EdgeSight Agent 5.2 from EdgeSight Agent 4.2 or 4.5 using a new MSI file. If you do not have the latest service pack installed for a prior version, install the service packs for the specific version before upgrading to EdgeSight Agent 5.2. Agent data files (agent database and log files) and registry key settings are retained during the upgrade.

Important: If agents are not upgraded to a minimum version of 5.2, data for the associated device cannot be uploaded to an EdgeSight 5.3 server, as described in "Agent Requirements" in [System Requirements for EdgeSight 5.3](#).

Direct upgrades of EdgeSight 4.1 agents are not supported. If you are using an EdgeSight 4.1 agent, you can first upgrade to a 4.2 agent and then perform a 5.2 upgrade. This will retain agent data and settings. If you do not need to retain data, you can uninstall the 4.1 agent and reinstall an EdgeSight 5.2 agent.

You can uninstall an agent using any of the following methods:

- Execute the `msiexec` command for the EdgeSight MSI with the `/uninstall` argument
- Right-click on **EdgeSight.msi** and choose **Uninstall** from the pop-up menu
- Use the Add and Remove Programs feature on the Control Panel

You may encounter an error during uninstallation indicating that files cannot be removed from the system. In most cases, clicking **Retry** will result in a successful uninstallation. After uninstalling an agent, reboot the target machine. If the machine is not rebooted, a subsequent attempt to install an agent will fail.

Note that the `DELETE_DATA_ON_UNINSTALL` property controls whether agent data files (agent database and log files) are deleted when the agent is uninstalled. The default setting is to delete agent data files. See [Installing EdgeSight Agents Using the Command Line](#) for more information.

Upgrading EdgeSight in a Virtual Desktop Environment

The following upgrade information relates to upgrades from EdgeSight 5.0 or 5.1 agents to EdgeSight 5.2 agents:

- If you have existing EdgeSight Agents running on virtual desktops, you must uninstall and reinstall the agents.
- The Agent Database Server can be directly upgraded. Any agent databases currently resident on the server are also upgraded. This ensures that no data is lost when EdgeSight for Endpoints Agents are replaced with EdgeSight for Virtual Desktops Agents.

Because all required components must be in place, and because some installation steps are dependent on previous actions, the following task sequence is recommended:

1. Uninstall the agents.
2. Upgrade EdgeSight Server.

3. Upgrade the Agent Database Server ([Installing the Agent Database Server](#)).
4. Install the new agents ([Installing the Agent](#)).

Managing EdgeSight

EdgeSight Agents

The EdgeSight Agent is a service that runs on an end-user device, virtual desktop, or XenApp Server and collects data, which it writes into a client-side database. The agent collects data, aggregates the data into a payload, and sends the payload to the EdgeSight Server. The following types of agents are available.

- **EdgeSight for Endpoints Agent**—Endpoint agent software is designed for the user desktop or laptop environment. The agents operate continuously and discreetly on user systems collecting performance, resource, application and network data. The data is collected and stored in a local database and uploaded to an EdgeSight Server on a scheduled basis. Data can also be displayed directly from an agent database for use in problem resolution
- **EdgeSight for Virtual Desktops Agent**—Virtual desktop agent software is designed to monitor virtual desktops based on XenDesktop 4.0 or higher. In addition to monitoring system, application, and network performance, it collects ICA channel data including XenDesktop multi-media counters, collects end user experience metrics, and alerts on XenDesktop session performance. Note that this agent does not provide monitoring of the Desktop Delivery Controller (DDC).

Agents store data in a remote database and file share, with the EdgeSight Server acting as a database broker.

- **EdgeSight for XenApp Agent**—XenApp agent software is designed for use on XenApp Servers. Data is collected and stored in a local database and uploaded to an EdgeSight Server twice a day. Data can also be displayed directly from an agent database for use in problem resolution. There are two levels of EdgeSight for XenApp Agent:
 - *Basic* agents require only that you have a XenApp Enterprise license available on your Citrix Licensing Server. The agent records information about client and server performance and application usage.
 - *Advanced* agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix Licensing Server. The agent records information about user sessions, client and server performance, application usage, and network connections.

EdgeSight Server

The EdgeSight Server collects data from the distributed agents and allows administrators to display the data to identify potential issues in the enterprise and to assist in problem resolution. The following components make up the EdgeSight Server:

- **Web Server**—The web server component accepts the data uploads from the agents and then displays performance and availability information in a wide range of standard reports through the EdgeSight Server Console.
- **Database Server**—The database server component stores the data uploaded from the agents and acts as the data source for Reporting Services.
- **Report Server**—The report server component generates performance and availability information in the form of reports. The report server uses Microsoft SQL Server Reporting Services.

In an environment where EdgeSight for Endpoint Agents are monitoring virtual desktops in a pool, additional components are required:

- **EdgeSight Agent Database Server**—This provides data storage for agents running on virtual desktops in a pool. The EdgeSight Web Server includes database broker components from which agents acquire a connection to an agent database server. The database broker components are installed by default.
- **Agent data file share**—The agent data file share provides storage for files such as log files and INI files which are not stored on the EdgeSight Agent Database Server.

EdgeSight Server Console

Administrators interact with the EdgeSight Server through the EdgeSight Server Console. The console provides a powerful and flexible tool for displaying availability and performance information from the data collected by the distributed agents. To access the console, open a web browser to the URL for the EdgeSight Server and providing credentials on the logon page. An administrator can access the console using the following URL:

`http://servername/edgesight/app/default.aspx`

The EdgeSight Server Console has the following components.

- **Tabs**—Use the tabs at the top of the content area to select the type of data you want to display or operation you want to perform. Most of the information in this guide pertains to the Configuration tab. The tabs are as follows:
 - **Getting Started**—This tab provides overview information for each tab. Click on each tab name to display descriptions of tab features. A checkbox allows you to disable the display of this tab on your subsequent logins.
 - **Monitor**—This tab allows you to perform real-time monitoring of performance counters on specified devices and to display information on alert conditions.
 - **Troubleshoot**—This tab allows you to perform real time troubleshooting using troubleshooting tools and real time reports. The real time reports display data directly from an agent database.

- **Plan and Manage**—This tab allows you to display summary reports which provide an overview of your environment. Summary information can be displayed for devices, XenApp servers, users, processes, Websites, or transactions.
- **Track Usage**—This tab allows you to display reports on usage of Citrix licenses, on published application launches and users, and on session duration.
- **Browse**—This tab allows you to browse or search lists of reports and to display reports. You can also display report properties and subscriptions.
- **Configure**—This tab allows you to edit your user profile, configure companies (including agent options, alerts, devices, and security), configure the server (including licensing, authentication, database grooming, and company creation), and monitor server status (including messages, jobs, services, and agent database broker activity).
- **Menu Bar**—Use the Menu Bar at the top of the content area to perform common operations on the current page, such as adding a page to your list of favorites, refreshing a page, or printing a page. When displaying a report, you can add the report to the list of favorite reports or subscribe to the report.
- **Filter Bar**—Once a report is selected, use the Filter Bar to filter report data. Depending on the report selected, filter by department, group, time period, process, device, user, site, and other data types. Filter data to isolate information based on particular classes of processes, devices, or users and to quickly identify problems or trends. You can also filter data on non-report pages such as the Current Alert List or the administrative and configuration pages. Click Go to apply filter parameters.
- **Help Link**—Click the Help link at the top right of the console to invoke context-sensitive online help. In addition to context-sensitive help, the help system also provides reference material, such as a glossary of report metrics and a definition of SQL views.

License Server

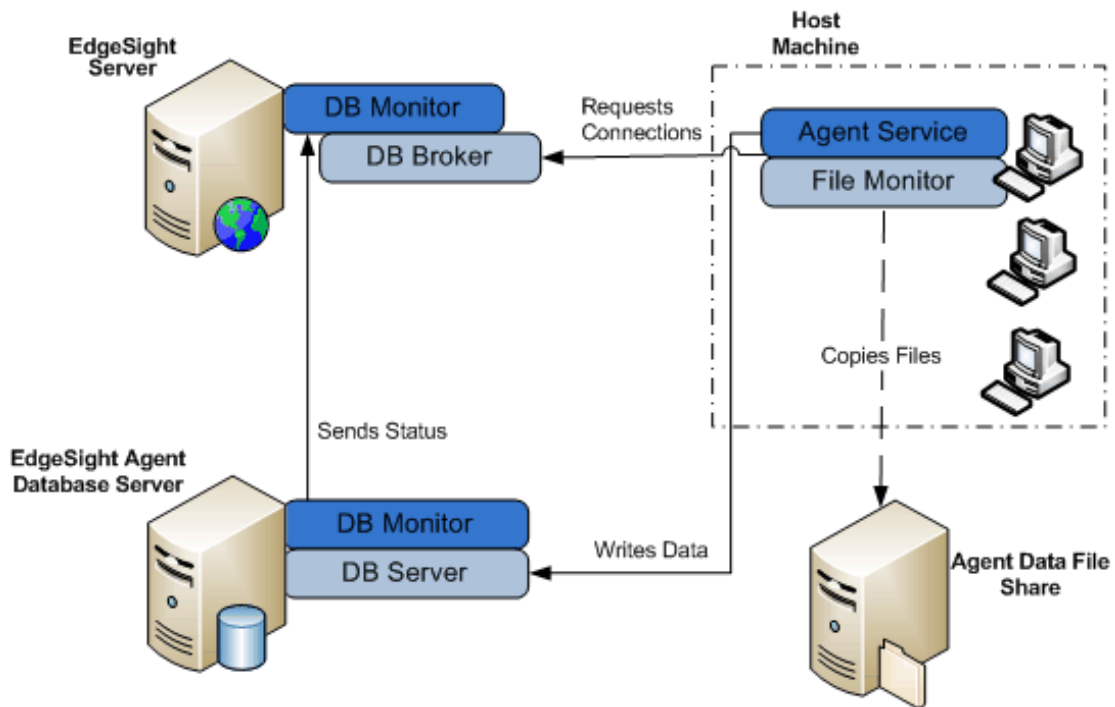
Citrix License Server for Windows 11.6 or higher is used to supply licenses authorizing EdgeSight Agents to upload data to an EdgeSight Server. The license server can be anywhere on the network as long as it can be reached from the web server component of the EdgeSight Server and by the XenApp Agents. A single license server can be shared by multiple Citrix products, including multiple EdgeSight Servers.

Note: The license server and the EdgeSight license files should be in place before deploying EdgeSight in order to avoid delays in uploading data.

Separate licenses for XenApp Agents and Endpoint Agents must be obtained, even if both types of agents are associated with the same server. All agent license files (for example, CESEP_*.lic) must be placed in the MyFiles folder of the license server directory on the EdgeSight Server.

EdgeSight Components Required for Virtual Desktop Monitoring

When using EdgeSight to monitor virtual desktops where data is not persisted across reboots, additional components are required for storing agent data. The following figure shows the relationship between these components and the systems being monitored:



The components required for virtual desktop monitoring include the following:

- **EdgeSight Server**—Each EdgeSight Server installation includes database broker and database monitor components which supply database connection information to EdgeSight agents running on virtual desktops in a pool and listen for EdgeSight Agent Database Server registration and status.
- **EdgeSight Agent Database Servers**—The database servers store data collected by EdgeSight agents running on virtual desktops. The database monitor on each server communicates with EdgeSight Server to announce its availability and update status at regular intervals.
- **Agent Data File Share**—The file share stores agent files which are not stored in the EdgeSight Agent Database Server, such as log files and INI files.
- **EdgeSight Agents**—The EdgeSight Agents collect performance data for the virtual desktops or systems on which they are installed. During agent installation, you specify which EdgeSight Server is to supply database connection information and the path to the agent data file share.

The EdgeSight components function within a larger environment which includes Citrix Provisioning Server and may include XenServer.

For more information on using the EdgeSight Server Console to monitor the status of pools, agent database servers, and database broker messages, see [Displaying Agent Database Broker Status](#).

Terms and Concepts

A *company* is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies. Companies are broken down into *departments*. Departments are organized as a hierarchical tree with a default root department (All), and device-specific subdepartments (XenApp Farms, XenDesktop Farms, and Endpoints) which are created on installation. The structure of the XenApp Farms and XenDesktop Farms subdepartments is determined by the farms being monitored and cannot be changed using the EdgeSight Server Console. Additional Endpoint subdepartments can be created automatically as agents register with the server, or can be created manually. Configuration information is associated with agents based on their department. Each department corresponds to a set of systems running EdgeSight Agents. These systems are referred to as *devices*.

In addition to the department structure, you can organize devices by custom *groups*. A custom group is a user-defined collection of devices. Membership in a group can be based on the associated departments, device characteristics, or queries.

In addition to groups of devices, you can also create *user groups* which are collections of XenApp, XenDesktop, or endpoint users. Many reports containing data on user experience can be filtered by user groups, allowing you to monitor system performance for a group of users with specific characteristics.

EdgeSight Console *users* log on to the console to display reports or perform administrative tasks. (Note that reports use the term user to indicate a XenApp or XenDesktop user associated with a session.) Each console user is assigned a *role* (such as the default roles of Administrator or Report Viewer) which has an associated set of *permissions*. These permissions determine what actions a user can take and what pages are displayed on the console. For example, a user with a role of Report Viewer can display reports but cannot display pages under the Company Settings or Server Settings folders and perform administrative functions on the server.

Users can display reports from the console or can receive them based on a *subscription* which specifies the distribution of a report by email or to a file share. (This is an effective means of distributing targeted information to people in the organization without requiring them to log on to the console.) Subscriptions are distributed based on a defined schedule.

Agent Types and Processes

EdgeSight provides the following types of agents:

EdgeSight for Endpoints	Endpoint agents provide monitoring and data collection for physical endpoint devices.
EdgeSight for Virtual Desktops	Desktop agents provide monitoring and data collection for virtual desktops based on XenDesktop 4.0 or higher.
EdgeSight for XenApp	<ul style="list-style-type: none">• Basic agents require only that you have a XenApp Enterprise license available on your Citrix Licensing Server.• Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix Licensing Server.

Agent Processes

The EdgeSight Agent includes the following key processes:

Citrix System Monitoring Agent Service	<ul style="list-style-type: none">• Collects data (resource usage, events, and hardware changes) from an end-user device, XenDesktop instance, or XenApp server.• Communicates with the EdgeSight Server on port 9035 for configuration downloads and payload uploads.• For an agent in a pooled desktop environment, requests a connection to a remote database.
Firebird Service process	<ul style="list-style-type: none">• Stores the data from the user device or XenApp server in the local agent database.
File Monitor process	<ul style="list-style-type: none">• Copies files to and retrieves files from an agent data file share, if an agent is installed on virtual desktops in a pooled environment.

The system overhead for the agent processes includes the following. Note that these are average values and may vary based on the individual machine and environment. (Note that agents installed on virtual desktops have smaller disk space requirements because they use a remote database for storage.)

- 1-2% CPU overhead
- 30-35 MB working memory
- 200 KB per day network utilization
- 40 to 250 MB of disk space

Agent Data Collection

Data collection is typically performed during hours of normal system usage to ensure that the data collected is an accurate representation of system availability and performance, without being skewed by large amounts of idle time. Some metrics, such as critical application and service resource statistics, are only collected when the user is actively using the system. The following types of data are collected and stored in the agent database:

- Performance data
- Event-driven data
- XenApp and XenDesktop data

Performance Data

Performance data includes polled data for system metrics, such as CPU or memory usage, that is a product of normal system operation. EdgeSight collects data including but not limited to the following:

- CPU utilization
 - CPU usage over a period of time
 - CPU comparisons on multiple devices
 - CPU utilization tracking
 - Which processes are consuming the most CPU
- Memory utilization
 - How much RAM is being consumed
 - Which applications are consuming the most memory
 - Which machines have the least free memory
- Disk utilization
 - How much hard drive space is available
 - Which systems have potential hard disk issues
 - Which machines have the least free disk space

Event-Driven Data

Event-driven data includes metrics that are generated by an event occurring on the user system, for example, when the user invokes and starts to use an application or when a socket connection is made. EdgeSight collects data including but not limited to the following:

- Application issues (errors, crashes, and non-responsive applications)
 - What error message appeared

- When the error occurred
- How many times the error occurred
- Which system generated the error
- What else was running on the system at the time of the error
- Application usage (especially useful for tracking license compliance)
 - How long was the application running in memory
 - How much active or idle time has elapsed
 - What applications are being used by which users
- Network connection
 - Response time for network communications
 - Average speed of the network
 - Amount of network volume being utilized
 - Round trip time for certain connections
 - Systems experiencing the most delay
 - Applications generating the most volume
 - Slowest responding servers
 - Protocols in use on the network
 - Sites visited and new sites

XenApp and XenDesktop Data

XenApp data includes, but is not limited to, the following:

- End User Experience Monitoring (EUEM) data, including session performance, ICA round trip, and client and server startup metrics. This ICA round trip data replaces the session latency data collected by older agents.
- Session activity, such as active, inactive, and total sessions
- Session auto-reconnects
- ICA session input and output bandwidth for audio, video, printers, and file operations
- IMA service state and availability
- Resource usage, such as memory and CPU, for groups of users
- Session network delay and round trip time for groups of users
- Published application launches and unique users, by farm or by user group

- Active Application Monitoring data, such as application test response times and application test failures

XenDesktop data includes, but is not limited to, the following:

- ICA channel data including XenDesktop multi-media counters
- End User Experience metrics
- XenDesktop session performance

Agent Data Aggregation

Agent data is aggregated in the following way:

- Data is collected and then stored every 5 or 15 seconds in the local agent database. Endpoint data is stored every 5 seconds, and XenApp data every 15 seconds.
- Every twenty minutes, the collected data is aggregated into 5 minute increments and placed in a new location in the local agent database.
- Once a day, the 5 minute increments are re-aggregated into one hour increments and then uploaded to the EdgeSight Server based on the configured upload schedule.
- Data is stored for 3 days in the agent database so that historical information can be displayed. After 3 days, the data is groomed from the agent database; however, the time that the data is retained can be extended by editing the agent properties.

If the agent software is installed on a mobile device, or the device is unable to connect to the EdgeSight Server, aggregated data is retained for up to 5 days for XenApp servers and 29 days for endpoints and virtual desktops, or until the device is able to upload to the server. You can configure the data retention time as required. For more information, see the Agent Properties Wizard topic in online help.

Agent Data Upload

When the agent is first installed, it registers itself with the server and obtains information about when data is scheduled to be uploaded to the server and what data is required by the server.

Using the default Performance Upload worker configuration, data is uploaded from the agent database to the EdgeSight Server. Endpoint agents upload once a day by default, XenApp agents upload twice a day, and Virtual Desktop agents upload every hour and a half. You can configure agents to upload more frequently if required. For instance, a mid-day data upload can be scheduled to evaluate morning activity. For more information on worker configurations, see [Configuring, Scheduling, and Running Workers](#).

A typical data upload size for an EdgeSight for Endpoints agent is 80KB. EdgeSight for XenApp agent data uploads are typically larger due to the greater amount of data collected and can reach 300KB. These data upload sizes depend on a number of factors such as the agent properties and the usage profile of the system hosting the agent.

The data upload process can be summarized as follows:

1. The EdgeSight Agent contacts the EdgeSight Server to find out what data is requested based on when the last successful upload occurred.
2. The agent queries the local database and aggregates the polled payload data into one-hour increments.
3. The payload data is compressed and sent to the web server components of the EdgeSight Server using either HTTP or HTTPS. (HTTPS is used if the agent is configured to connect to the server using SSL. SSL support must be enabled on the server, and a valid SSL certificate issued by a trusted certificate authority must be present on the server running the EdgeSight Website.)
4. The payload data is stored in the local data folder from where it is retrieved and processed by the EdgeSight Script Host (RSSH).

Administrative Tasks and Roadmap

In order to perform administration tasks, you must be assigned the Administrator role or you must have been granted administrative privileges. Administrative tasks are grouped at the company level and the server level.

In order for an administrator to view and edit server-wide settings, they must be granted the Manage Server Settings permission. This permission is automatically granted to the Superuser created during installation. For additional users, it must be explicitly granted when the user is created or edited rather than by role assignment.

Company settings only affect a single company, while server settings affect all companies resident on the server. Company settings include both server and agent settings.

When you perform the initial configuration of EdgeSight using the Post-Installation Wizard, you explicitly specify a number of critical operating parameters for EdgeSight Server. These include an initial (or root) company, a Superuser account that can access all companies on a server and can create new users, email settings used to send server notifications, and a port for use in communication with the license server. In addition to these explicitly set parameters, there are many default settings which enable EdgeSight to be fully operational as quickly as possible. This section outlines the remaining tasks that you perform after installation and initial configuration to reach full operational status. Some of these tasks differ depending on your environment, such as the type of systems being monitored and whether you are using the default email authentication provider or Active Directory for authenticating users.

Configure Authentication for Reporting Services

Microsoft SQL Server Reporting Services must be installed and configured in order to generate and display EdgeSight reports. Once EdgeSight is installed, you must configure credentials used to authenticate the EdgeSight Server to the Report Server. For more information, see [Configuring Reporting Services](#).

Add Roles

Before adding users (people who can log on to the EdgeSight Server Console), it is recommended that you add any roles that will be required to determine what actions they can perform on the console. For more information on defining roles, see “Creating Users and Assigning Roles” in [Managing Roles](#).

Add Authentication Provider

If you want to automatically create users based on an Active Directory tree, you must add an AD authentication provider. Before creating a new provider, make sure you have the LDAP path for your AD authentication provider available. For more information on adding an AD authentication provider, see [Managing Authentication Providers](#).

Add Users

If you are using the default email authentication provider, you can add users and assign roles to them from the EdgeSight Server Console. For more information, see “Creating Users and Assigning Roles” in [Managing Roles](#).

Adjust Agent and Worker Configurations

Depending on your environment, you may need to adjust which agent and worker configurations are applied to the devices in a department. Default agent and worker configurations are supplied for endpoint, XenApp, and virtual desktop systems. Verifying that devices are in the correct departments and that the appropriate agent and worker configurations are applied to these departments helps ensure efficient EdgeSight Server operation. It is recommended that you use the default configurations for a period of time and then adjust the configurations if required to resolve data collection issues. For more information on agent properties, see [Setting Agent Properties](#). For more information on worker configurations, see [Configuring, Scheduling, and Running Workers](#).

Managing Company Settings

Company settings allow you to manage the configuration of companies hosted on a Citrix EdgeSight server. All company settings are located on the Configure tab under the Company Configuration menu item.

Company settings allow you to perform the following tasks:

- Managing User Profiles
- Managing Company Properties
- Managing Departments, Devices, and Groups
- Managing User Groups
- Managing Roles
- Creating Users and Assigning Roles
- Managing Access to XenApp Farms
- Creating Alert Rules and Actions
- Managing Application Categories and Vendors
- Managing Reports
- Managing IP Ranges
- Managing Real-Time Dashboard Configurations
- Setting Agent Properties
- Configuring, Scheduling, and Running Workers

Managing User Profiles

Each EdgeSight Server Console user has a profile stored on the server which includes name, title, and contact information. Users can edit their own profiles. Click on **My Settings > Profile** to display the profile matching the username under which you logged in to the console.

You can display the profiles of other EdgeSight Server Console users on the Users page (**Company Configuration > Security > Users**). For more information on the creating and managing users, see "Creating Users and Assigning Roles" in [Managing Roles](#).

Managing Company Properties

A company is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies. If there are multiple companies on the server, use the Company drop-down menu at the top right hand corner of the console to switch between companies. Company settings are administered separately from server settings, allowing server administrators to control which users are authorized to display reports or change settings for a specific company. To display company settings, navigate to **Company Configuration > Settings**.

Time Zone and Daylight Savings Time

There is a time zone for each company on an EdgeSight Server. The time zone is used by the server when displaying times in reports, when scheduling and running maintenance jobs, and for timestamps associated with events, such as alerts and upload times. All data for a company is consolidated based on the day boundary for that time zone. This ensures greater data consistency when agent machines are in a number of different time zones. In addition to the time zone setting, you can specify whether or not to adjust times for Daylight Saving Time.

When EdgeSight is installed, an initial company must be created, including a time zone setting. The Company Settings page allows you to change the company time zone as required. When creating new companies using the console, you must specify a time zone.

Agent Registration Settings

Agent registration settings control how EdgeSight Agents make themselves known to the server. (Agents initiate communication with the server in all cases except for explicit requests for agent data, as in the case of displaying a real time report from the console.) Use the menus to enable or disable each setting, then click **Save Changes** to apply the new settings. Enabling all the client registration settings is recommended. Allowing EdgeSight software to handle agent registration, department creation, and duplicate instances can save you time and effort that would otherwise be spent on manually resolving these events. The following table describes how each setting affects client registration.

Registration Setting	Controls...
Automatically Register Agents	When an agent connects to a server, it passes Company and Department configuration information. If this information matches an existing company defined on the server and this setting is enabled, then the agent is enlisted into the company. Otherwise, the agent is an unmanaged instance and only appears on the Unmanaged Devices page. (For more information on moving unmanaged devices to a company and department, see Handling Unmanaged Devices .)

Automatically Create Departments	When an agent connects to a server, it passes Company and Department information. If the Department does not exist, then it will be created if this setting is enabled. If the setting is not enabled, the device is placed in the root department for the company. (For more information on departments, see Managing Departments, Devices, and Groups.)
Coalesce Duplicate Instances	<p>If an EdgeSight Agent database becomes corrupt, as part of the repair process the machine will be matched up with its historical data on the server if this setting is enabled. If the feature is disabled, then there will be a duplicate record of the device in the system. You are notified of the creation of a duplicate record by a message on the Messages page similar to the following:</p> <pre>EdgeSight - New Instance (DUPLICATE) - Machine: 'sysname' Domain: 'domain_name'</pre> <p>An internal identifier (a globally unique identifier or GUID), rather than the machine name, is used to match duplicate instances.</p>

Managing Departments, Devices, and Groups

Companies are broken down into departments. Departments are organized as a hierarchical tree with a default root department (All), and device-specific subdepartments (XenApp Farms, XenDesktop Farms, and Endpoints) which are created on installation. Endpoint subdepartments which can be created automatically as agents register with the server, or created manually by a user with administrative privileges. Each department corresponds to a set of devices (systems running EdgeSight Agents).

In addition to the department structure, you can organize devices by custom groups. A group is a user-defined collection of devices. Membership in a group can be based on the associated departments, device characteristics, or queries.

Managing Departments

The root department (named All by default) and the XenApp Farms, XenDesktop Farms, and Endpoints subdepartments are created during the installation of EdgeSight. You cannot delete these default departments. The root department uses the Endpoint default configuration for agent properties and agent workers. Alert rules must be explicitly associated with the root department. The structure of the XenApp Farm subdepartment is determined by the XenApp Farm structure, and the structure of the XenDesktop Farm is determined by the Desktop Delivery Controller. These subdepartment structures cannot be changed using the EdgeSight Server Console.

Endpoint subdepartments can be automatically created based on information from agents as they register with the server. When an endpoint agent connects to a server, it supplies Company and Department information. If the Department does not exist, then it will be created if the Automatically Create Departments setting is enabled, as described in “Agent Registration Settings” in [Managing Company Properties](#). If the setting is not enabled, the device is placed in the root department for the company.

Use the Department page to create, edit, or delete endpoint subdepartments and also to associate alert rules and configuration settings with devices in the department. Alert rules, worker configurations, and agent properties can be created or edited any time, but they are not used until explicitly associated with departments. See “Departments” in the console online help for detailed instructions on creating and editing departments and mapping rules and configurations to departments.

Managing Devices

The devices displayed on the Devices page represent systems which are running EdgeSight Agents and have successfully registered with the server. Devices can be XenApp servers, desktops, laptops, or terminal servers. They can also be physical or virtual machines. If you have selected the default agent registration settings, which allow automatic agent registration and department hierarchy creation, the list of devices is automatically populated with all agents configured to communicate with the server. Once an agent running on a device has registered with the server, you can move the device to another department as required. (See “Agent Registration Settings” in [Managing Company Properties](#) for more information on agent registration.)

The device name, domain, and last upload time for the device are always displayed. The remaining device information can be selected using the **Show** drop-down menu. Refer to online help for a complete list of information available. Note that the last upload time shown in the Devices table is the last time a payload from that device was processed by the server. This is a useful indicator that agents are properly uploading data to the server.

If a specific device does not appear on the list, this may indicate a problem with company/department assignment. Navigate to **Server Configuration > Unmanaged Devices** to display a list of devices which have registered with the server, but are not associated with a company or department.

Creating and Using Custom Groups of Devices

You can create custom groups of devices on EdgeSight Server. Groups are collections of devices based on departments, a selected set of individual devices, SQL queries, or a combination of these criteria. When EdgeSight is installed, several commonly used groups are provided, such as “Citrix XenApp” and “All Windows Server 2003.” A group can be defined using one or more of the following criteria:

- All of the devices in one or more departments
- A selected set of individual devices within a department or across departments
- A selected set of individual devices to be excluded from the group
- A set of individual devices selected using an SQL query run against the EdgeSight database

Groups allow you to isolate and display data based on specific device characteristics, helping you to resolve cross-department system management issues. The following examples illustrate cases where custom groups are useful:

- You are asked to evaluate the performance enhancements to be realized from moving to a new operating system. Create custom groups of devices based on the devices running the current and new operating systems and compare group performance over time.
- You are asked to determine the effectiveness of a software patch prior to enterprise-wide deployment. Create custom groups of devices with and without the patch installed and compare the performance and availability of the target application over time.

- You are asked to closely monitor a group of devices at risk of problems due to known hardware issues. These devices reside in several different departments. Create a custom group of target systems and filter incoming alerts using the group.

Groups have the following attributes:

- **Name**—A unique name identifying the group. The name should be descriptive enough to allow a console user to readily select the correct group from a drop-down menu.
- **Expiration period**—A selected time period after which the group expires and is deleted. This feature facilitates the management of groups created for short-term projects with a set duration, such as the evaluation of software. Groups can also be set to never expire. No explicit notification is sent before group expiration.
- **Refresh period**—A selected time interval after which the device cache for the group is refreshed. Device cache refreshing ensures that devices which meet the criteria for group membership are detected and added to the group.
- **Public/Private**—Groups can be public (available for use by all console users who have a role of Administrator) or private (available only to the user who created the group). Private groups for a subset of all console users are not currently available.
- **Member Type**—Groups can be populated based on one or more of the following criteria: department, a selected set of devices, or an SQL query. Departments can be included as a single department or as a department tree, which includes the selected department and all subdepartments. A set of devices can be selected from a list of existing devices or imported from a comma separated value (CSV) file. Basing groups on an SQL query is an advanced capability that will probably only be necessary in certain cases where you require a set of devices based on a narrow set of criteria. In these cases, you will need to use database tools to expose the database structure.

Note: It is good practice to set the expiration period to a value which reflects the lifetime of the related task. For example, if you are evaluating a patch and need to collect 3 weeks of data, choose 1 month as the expiration period. If you need additional time to collect data, you can always edit the expiration period. Setting realistic expiration periods helps keep the list of groups manageable for you and for other users (if the groups are public). In addition, because the group's device cache is refreshed at regular intervals, setting expiration periods helps manage system resources wisely.

For detailed instructions on creating custom groups, see the “Groups” topic in online help.

Managing User Groups

In addition to groups of devices, you can also create groups of users. The user group capabilities of EdgeSight enable you to create collections of users by selecting users by username, IP address or IP range, or by running a SQL query against the EdgeSight database. The users can be XenApp, XenDesktop, or endpoint users. Many reports containing data on user experience can be filtered by user groups, allowing you to monitor system performance for a group of users with specific characteristics.

To manage user groups, go to **Company Configuration > User Groups**. User groups have the following settings: name, public/private setting and members. User groups can be public (available for use by all console users who have a role of Administrator) or private (available only to the user who created the group).

Members can be explicitly selected from a list of users (identified by user name or by IP address), selected based on a range of IP addresses, or selected based on a SQL query run against the EdgeSight database. Note that when a user group cache is updated, if the group membership is controlled by a query, the query is rerun and any new users matching the query will be added to the user group. This greatly simplifies the maintenance of query-based groups. For detailed instructions on creating user groups, see the “User Groups” topic in online help.

Managing Roles

When users are configured on a Citrix EdgeSight Server, they are assigned one or more roles. Roles define a set of permissions which control what operations a user can perform. An EdgeSight Administrator can define new roles and edit existing custom roles. There are two non-editable system-defined roles, Administrator and Report Viewer. The Administrator role has all permissions and the Report Viewer has a limited set of permissions that enables the user to view all EdgeSight reports. Creating a role involves selecting the permissions associated with the role. Optionally you can assign the roles to existing users. For more information on creating roles, see the "Add New Role" topic in online help.

Creating Users and Assigning Roles

A user is an individual (or group of individuals) for which an account is created on the EdgeSight Server Console. When the initial server configuration is performed, a Superuser account is created. This account has access to all companies hosted on the server and can create other users. The Superuser can create an account for one or more administrators for a company, and then the administrators can continue with the creation of additional user accounts as required. You create and manage users on the Users page (**Company Configuration > Security > Users**). After you create a user, an email is sent to the user which includes login instructions and a temporary password. For detailed instructions on creating users, see the "Users" topic in online help.

User access to the EdgeSight Server Console is controlled through login authentication, while a user's capabilities to display and edit data and perform administrative operations are controlled by a system of roles and permissions.

User logons are authenticated by either the built-in EdgeSight provider (user email address and password) or Active Directory (AD). (See [Managing Authentication Providers](#) and the "Authentication" topic in online help for information on creating an AD authentication provider.)

New users can be assigned one of the built-in roles (Administrator or Report Viewer) or assigned a previously created custom role. Each role is defined by a set of permissions. Assigning a role to a user automatically grants the associated permissions to that user. For detailed instructions on creating roles, see the "Roles" topic in online help.

To display the full set of permissions which can be assigned using a role, navigate to **Company Configuration > Security > Roles**, click on the information icon for the Administrator role, and then select the **Permissions** tab in the detail pane.

Note that the Manage Server Settings permission does not appear on the list. This permission must be explicitly granted when a user is created or edited rather than granted by role. While other permissions allow users to perform operations at the company level, this permission allows a user to view server-wide settings.

Managing Access to XenApp Farms

Use the Farm Authentication page to create and maintain default credentials used in accessing XenApp farms. The credentials consist of a farm name, user name, password, and domain name. The credentials are used when querying farms directly while searching for active sessions. (The report is accessible from the **Troubleshooting** tab.)

To find user sessions and display this report, you must select a query method. The **Query one or more farms directly** method is the recommended method for locating an active session for a specific user. Because this method requires existing credentials for logging in to the selected farms, you must specify a set of credentials for each farm in order for reports to be generated based on this query method.

Note: Credentials cannot be saved for a department which has no devices.

Creating Alert Rules and Actions

This topic outlines basic real-time alert concepts and provides strategies and guidelines for implementing alert rules in EdgeSight. For detailed instructions on creating real time alerts and actions, see the “Alert Rules” and “Alert Actions” topics in online help.

Real-time alerts allow you to monitor mission-critical applications and devices and notify designated people in your enterprise in the event of a problem. By default, alert data and statistics are collected by the agent on each desktop and uploaded to the server on a daily basis. When you explicitly configure an alert by creating an alert rule, you are requesting real-time notification that a specific alert condition has occurred.

The purpose of real-time alerts is to provide timely notification of critical events that require immediate attention. For example, alert rules ensure that data is available for display in the Farm Monitor. The Farm Monitor allows you to browse through a XenApp Farm and display real-time alerts and system context for one or more devices. When developing an alert rule strategy, ensure that alert rules are only created for events that have an associated resolution. Real-time alerts are not intended for data collection; agents collect relevant data whether or not an alert rule exists, and historical reports are the most effective means of displaying availability and performance data.

Proper alert configuration is critical to effective real-time alert notification on the health of distributed devices and applications. It enables you to quickly identify which issues are truly critical and require immediate attention and which issues can wait. In order to achieve an effective alert configuration, you must have an alert strategy in place. When designing your strategy, you will need to do the following:

- **Identify which applications are critical to your business or service** - Focus on critical applications and define alerts only for problems that must be resolved in a short period of time.
- **Identify which departments have mission-critical applications running on their systems** - Associate alerts only with the departments or groups where the alert condition is most critical. This allows you to isolate and respond to problems that are relevant to a specific portion of your business.
- **Identify which alert types are most important** - Some alerts, such as NT log alerts, are generated in large numbers by some applications and are generally transparent to the end user. As a result, prior to defining an NT log alert, verify the risk level of the alert condition by examining historical alert reports.
- **Identify what response is required to resolve specific alerts** - Responses may include performing a specific set of actions or notifying responsible individuals in the associated department. If no response can be identified for a condition, the event does not require a real-time alert.
- **Identify who is responsible for responding to the alert** - Determine who should respond to a specific alert condition.
- **Establish and publish guidelines for alert rule creation** - Determine who is responsible for new alert rule creation. Define best practices, such as creating descriptive names

for alert rules and avoiding duplicate alert rules. A user must have the Manage Alerts permission in order to create or edit an alert rule.

Once you have established an alert strategy, you can configure the required real-time alerts using the Alert Rules page in the EdgeSight Server Console (**Company Configuration > Alerts > Rules**).

Alert Features

A number of features enhance the ability to configure alert rules specific to a condition warranting an alert, and thus reduce the number of extraneous alerts generated by the agent. These precise alert rules should result in an actionable response if the alert is ever generated. The following is a list of some of the improved scenarios:

- Performance alert rules can be specified on complex parameters. For example, send a System Performance alert if the CPU is over x% and there is less than y free memory on the machine.
- Application alert rules can be defined to specify the company name of the process from which to generate alert rules. For example, if a process written by the specified company crashes, send a Process Fault alert to the company's internal support team.
- Windows Event Log alert rules can be specified to include the application and event writing the event to the event log. For example, if a group policy violation occurs, send an alert to the Security team.
- Negation logic (implemented as a **Not like** checkbox) can now be used in the definition of certain alert rules. For example, send an application terminated alert notification only if the terminated process was not written by the Internal Tools Team.

Alert Categories and Types

Real-time alerts can be broken down into two distinct categories: event driven and polled. Event driven alerts are generated whenever the associated event occurs in the system, while polled alerts are based on queries of the agent database on a periodic basis. In general, polled alerts are used as notifications of performance problems with an application, a system, or the network. For a description of how polled alerts function, see "Sampling, Polling, and Re-alerting Parameters" later in this topic.

When setting up alert rules using the Alert Rules Wizard, alerts are grouped into the following types based on the type of event or condition with which they are associated:

- Application alerts
- System alerts
- Network alerts
- XenApp performance alerts
- XenApp error alerts

- Session performance alerts
- XenDesktop error alerts

To help ensure that real-time alert data is available for XenApp Servers, the following alerts are preconfigured and assigned to the XenApp Farms subdepartment:

- Configuration Logging Database Unavailable
- Farm Data Store Connection Failure
- Health Monitoring and Recovery Action Failure
- Health Monitoring and Recovery Test Failure
- IMA Service is Unresponsive
- License Server Connection Failure
- Number of Servers in a Zone is Too High
- Published Application Concurrent Usage Limit
- Session in Down State
- Terminal Server Client Connection Error
- Terminal Server License Server Discovery Failure
- Zone Data Collector Election Triggered
- Zone Elections Too Frequent

The parameters for these alerts can be edited. Descriptions of each alert rule and parameter set is provided in the Alerts Rule Creation Wizard.

Active Application Monitoring Alerts

The EdgeSight Server Console displays real-time alerts received from Citrix Active Application Monitoring (AAM) software. This software allows you to record and create virtual user scripts and define tests. When the tests are run, virtual user ICA sessions are generated on the target XenApp servers. The results of the tests provide application response and availability information.

Important: The EdgeSight for XenApp Agent 5.0 or later running in Advanced Mode is required for the generation of Active Application Monitoring alerts.

The Active Application Monitoring alert rules are as follows:

- The Application Response Failure alert is generated when a monitored transaction has failed.
- The Application Response Time alert is generated when the time to execute a monitored transaction has exceeded the specified threshold.

These alerts are grouped under XenApp Performance alerts. For more information on installing the software, see [Install and Configure](#). For more information on creating and launching tests, see the online help included with the Active Application Monitoring software.

Notes on Specific Alerts

The following information on specific alerts is provided to help you understand under what conditions these types of alerts are triggered.

- **New process alert** -The new process alert only fires for processes which are used for the first time after the New Process Grace Period has expired. The grace period is set in the agent properties (for more information, see [Setting Agent Properties](#)). For example, the default grace period on XenApp agents is 7 days. If you install an agent and then start a process, the agent records this as a process, but not as a new process because the agent database is less than 7 days old. Once the database is more than 7 days old, then any new process (any process that is not already in the agent database) being run will trigger an alert. This avoids a large group of alerts being triggered at once because an agent was installed. Note that the grace period is relative to the agent database age, not the actual date of initial agent installation. If an agent database is recreated for some reason, then the grace period is reset.
- **Process hung alert** - This alert type corresponds to the “not responding” alerts shown in reports. EdgeSight software uses the Windows API (the `IsHangAppWindow` call) to determine if an application is not responding. An application is considered to be not responding if it is not waiting for input, is not in startup processing, and has not called the `PeekMessage` function within the internal timeout period of 5000 milliseconds (5 seconds).
- **Process fault and process snapshot alerts** - These types of alerts may generate crash reports, if conditions on the managed device allow for crash data to be captured. In some cases, the system is unable to support the collection of data. In the case of process fault alerts and the resulting crash reports, there are several factors to consider:
 - If the crash file cannot be written, a message to that effect is logged to the `zcrash_loader` log file. Navigate to **Server Status > Server Script Host**, locate `es_zcrash_loader`, click on the menu icon and select **View Log**.
 - What is the age of the crash report? Crash report grooming is distinct from database grooming, and the time that crash reports are retained is controlled by the **Max Keep Days** setting. Navigate to **Server Configuration > Settings** and select the **Crash Processing** tab.
 - What is the limit for number of logs collected, and how much space is allocated to crash reports? (See **Server Configuration > Settings**.) If either the maximum number of crash logs or the maximum disk consumption limit is exceeded, application crash processing is disabled until the limit is increased. There is no reset operation that can be used to remove existing payloads.
- **Published Application Single Use Failure and Published Application Concurrent Usage Limit** - When enabling logging of connection control events on the XenApp server, the **Log over-the-limit denials** setting must be enabled to allow these SMA-based alerts to fire. (For XenApp 6 systems, use the **Logging of logon limit events policy** setting.) See the [XenDesktop](#) documentation for more information about configuring connection control events.

Sampling, Polling, and Re-alerting Parameters

Sampling is the periodic collection of data from the system being monitored. *Polling* is when the agent runs a query against the database to compare alert rule parameters to the data collected.

Each rule for a polled alert includes the following parameters:

- Percent of samples required
- Poll interval
- Re-alert

Most polled alert rules also include a non-editable Data sample window parameter, usually set to Poll interval plus one minute.

These parameters allow you to fine tune the frequency with which alerts of a specific type can be triggered. Sampling is performed as frequently as every 5 seconds, depending on the alert type. During sampling, the required data for the alert type is collected. When polling occurs, the collected data is compared to the conditions specified in the alert rule. The poll interval value determines how often polling is performed. The percent of samples required determines what percentage of the collected samples must be across the threshold (either higher or lower depending on the alert type) before an alert is triggered. If the alert defined by the alert rule has already been triggered within the re-alert period, another alert is not generated until the period expires and the alert condition reoccurs. The data sample window indicates how far back in time samples are included in the polling.

Note: The default poll interval is designed to provide timely generation of alerts while minimizing the impact of queries run against the database. Decreasing the poll interval (increasing the frequency with which queries are run) can have an adverse effect on system performance and should be done with caution.

Polled Alert Example

The following illustration shows an alert rule for detecting system slowdowns due to high CPU usage.

Rule Type:	System Slowdown
Rule Name:	System slowdown due to high CPU time
Standard Parameters	
• CPU time (percent)	40
• Processor queue length	
Advanced Parameters	
• Data sample window	Poll interval plus one minute
• Percent of samples required	10
• Poll interval	90 seconds <input type="button" value="v"/>
• Re-alert	Every poll interval <input type="button" value="v"/>

The alert functions as follows:

- EdgeSight Agent software samples the percentage of CPU time used. For the purposes of this example, the sampling rate is assumed to be every 5 seconds.
- Every 90 seconds, the software polls the sampled data to see if the percentage of CPU time has exceeded 40 percent in at least 10 percent of the total number of samples. Because the data sample window is defined as the poll interval (90 seconds) plus one minute (60 seconds), the samples gathered over the last 150 seconds are included. This means that 30 samples will have been gathered. If 3 or more samples out of 30 have a percentage of CPU time used over 40, an alert is generated.
- The re-alert parameter is set to **Every poll interval**, so if the percentage of CPU time exceeds the threshold in the data included in the next polling, another alert is generated.

When to Configure a Real-Time Alert Rule

EdgeSight does not require that you configure certain alert types for the EdgeSight Agent to collect data on the conditions which would generate the alert. If you are configuring an alert rule, you should only do so if you are in a position to respond to the alert within a matter of hours. If there is no appropriate response to the alert condition within several hours from alert generation, a historical report should be used to determine if an item of significance has occurred. Creating excessive numbers of alert rules can reduce the effectiveness of monitoring tools such as the Farm Monitor by flooding it with alerts, making it more difficult to identify truly critical events.

Performance Impact of Real-Time Alerts

Regardless of the alert rule type, there is some processing overhead for each rule configured for an agent. At a minimum, the agent must determine if the alert should be generated, and if so, it must send the alert to the server. In some cases, the agent must run an SQL query against the database to determine if alertable conditions are present; when the conditions are too broad, the agent is required to process large datasets to generate the alerts and send them to the server.

Since each alert rule configured for a given agent incurs processing overhead, and this processing may occur when the end-user is attempting to perform an important task, care should be taken to only configure alert rules which are both targeted and actionable. If there are concerns about the overall impact of the agent on a system, and a significant number of alert rules have been defined for that agent, you may want to reevaluate the defined rules to determine whether a historical report would be more appropriate than real-time alerts. The following list provides some general guidelines as to when a set of alert rules will negatively impact the end user:

- If more than 3 or 4 application or network performance alerts are defined.
- If process or network performance alerts are defined to trigger for common conditions, such as CPU usage over 5%.
- If process or network performance alerts are defined for very complex conditions (for example, populating a value for more than 2 or 3 performance thresholds). In these cases, the SQL queries run by the agent to determine if an alertable condition exists could themselves consume significant database cycles.
- If “Not Like” is defined on process or network performance alerts.
- If multiple textual “Like” or “Not Like” operations are defined on process or network performance alerts.
- If performance alert rules are defined which will never fire (for example, setting up a process performance alert for an application whose execution is blocked via group policy).

When Will the Server Show a Real-Time Alert?

Real-time alerts are not generated until the following conditions are met:

- Alert rules are created and assigned to a department.
- Devices have run the Init Worker or the Configuration Check Worker.
- The condition or event specified in the alert rule has occurred.

Note: Some XenApp alert rules are preconfigured and assigned to the XenApp Farms department as described in “Alert Categories and Types” earlier in this topic.

No alerts of any type are sent to the server until the agent has completed its startup sequence, which may take several minutes. Init and Configuration Check workers are run after the startup sequence completes, and worker execution is spaced out over several

minutes. Once an alert is generated, it is batched for delivery to the server. Alerts are batched for up to one minute, and assuming there is a network connection, sent to the server. If there is no network connection, or if the agent is stopped before the alerts can be sent, the queued alerts will not be received by the server, and will not be re-sent. (Real-time alerts are not guaranteed to be received by the server.) However, because the agent does not require real-time alerts to be configured for data collection, the alert condition is still captured and can be seen in the historical reports once a data upload occurs, even though they were not sent to the server as real-time alerts. Unsent alerts are also shown in the real-time alert reports that display data directly from the agent database.

Managing Alert Actions

The Alert Actions page (**Company Configuration > Alerts > Actions**) allows you to configure an alert action to be performed when a specific alert condition occurs. Alert actions can be used to:

- Send an email message.
- Generate an SNMP trap.
- Launch an external executable process on the EdgeSight Server.
- Forward alert data for Microsoft System Center Operation Manager (SCOM). For information on integrating EdgeSight alert actions with SCOM, see [Integrating EdgeSight Alerts with Microsoft System Center Operations Manager](#).

A single action may be associated with multiple alert rules. For example, there are multiple cases where an IT manager should be notified in case of an alert condition, so an action resulting in an email message being sent to the manager is associated with each applicable alert rule.

Note: Although only an EXE file can be launched using the “Launch an external executable process” alert action, you can launch cmd.exe and use command line arguments to call a non-EXE file such as a BAT or VBS file.

For information on creating alert actions, see the “Alert Actions” topic in online help.

Managing AlertSuppressions

The Alert Suppressions page (**Company Configuration > Alerts > Suppressions**) displays alerts that have been suppressed. As an administrator, you can edit or clear any alert suppression.

Any user can create an alert suppression from the Alert List located on the **Monitor** tab. Suppressions prevent the EdgeSight Server Console from displaying a specific type of alert based on source, device, or user, or by a combination of these criteria. Note that suppressions are only effective for the user creating them; other users are still able to view the alerts. For more information on alert suppressions, see the “Current Alert List” and “Alert Suppressions” topics in online help.

Managing Application Categories and Vendors

EdgeSight includes extensive application category and vendor listings for use in reporting by type of application or by software manufacturer. In many cases, the program fits into an existing category and matches an existing vendor. If necessary, you can create a new category or a new vendor for the new process. See the “Edit Categories” and “Edit Vendors” topics in online help for detailed procedures for creating and editing categories and vendors.

Managing Reports

EdgeSight provides a wide range of standard reports. These reports are available once EdgeSight Server has been installed and the connection to Reporting Services has been configured.

Managing Report Subscriptions

A subscription is a standing request to distribute a report in a selected format at specified times. Report distribution (subscription type) is done by email or by transfer of a file to a file share. Subscriptions can be public or private. Public subscriptions are displayed on the **Subscriptions** tab of the report details pane. Private subscriptions are only displayed to the subscription creator or an administrator. A subscription is a useful method of distributing targeted data to people in your organization without having to give them access to the EdgeSight Server Console. To display existing public subscriptions, navigate to **My Settings > Subscriptions**.

You can create a subscription while viewing the report using the **Subscribe** link in the filter bar. You can also create a subscription from any report list by displaying report properties and selecting the **New Subscription** button from the **Subscriptions** tab. See “Working with Reports” in online help for a detailed procedure for creating subscriptions.

By default, as an administrator, you are granted the required permissions to manage all subscriptions, both public and private. (See “Creating Users and Assigning Roles” in [Managing Roles](#) for descriptions of permissions and their relationship to roles.) This allocation of permissions allows you to control the distribution of data within your organization and also help you manage the impact on the Report Server.

Uploading Reports

Navigate to the Custom Reports page (**My Settings > Custom Reports**) and click on the **Upload a Report** button to transfer an RDL file for a custom report to the Report Server.

Always use a unique name when uploading a new report. Also, you should define and publish naming conventions for custom reports. Use the **Public** or **Private** radio buttons to determine whether the report is shared within your company. Public reports are displayed to all users unless the ability to view the report is restricted based on the selected permissions. Private reports are only displayed to the user uploading the report. The Public/Private attributes cannot be changed once the report is uploaded. To change any of these attributes, you must delete the report and then upload the report again.

If you make additional changes to the report, use the **Update** link on the Properties page to upload the RDL (Report Definition Language) file. For more information, see the “Custom Reports” and “Upload Custom Reports” topics in online help.

Managing IP Ranges

Setting IP ranges enables you to define the corporate network for use in filtering the network by corporate or external network hosts. Ranges of IP addresses defined on this page are represented as corporate network sites. This option is only required when the IP address you use is not defined in the private, non-external IP address range. For instructions on setting IP ranges, see the “IP Ranges” topic in online help.

Managing Real-Time Dashboard Configurations

EdgeSight provides a dashboard that allows you to display real-time information for specific devices and counters, based on a saved configuration. The dashboard is displayed on the **Monitor** tab.

Note: Devices must be running an EdgeSight Agent of version 4.2 or later in order to be displayed on the dashboard.

The Real Time Configurations page allows you to create and edit named configurations for the dashboard. Configurations include:

- A unique name
- Timeouts for queries and connections
- An update interval
- Counters to display for the selected devices

You can select a maximum of 20 devices and 8 counters for the configuration. See the "Real Time Configurations" topic in the online help for detailed instructions on creating and editing configurations.

Once a configuration has been created, it is added to the drop-down menu on the Dashboard page, allowing users to select the configuration for viewing on the dashboard. The dashboard is populated with data based on direct queries to managed devices; no dashboard data is stored on the server.

Setting Agent Properties

The EdgeSight Agent stores configuration data in two locations. The Windows registry on the managed device is used to store configuration items which are machine specific and are required for successful communication with the EdgeSight Server. For example, the name of the company the agent belongs to, the name of the server to contact, and any proxy information required to perform the communication are all stored in the registry. All other configuration items are stored in the EdgeSight Agent database. When the agent is running on virtual desktops in a pooled environment, the agent database is located on a remote server.

The items stored in the Windows registry are typically set once, and are supplied during agent installation. All other configuration items are supplied by the associated EdgeSight Server, and any changes in configuration are performed using the Agent Properties page. By default, an agent obtains its initial configuration shortly after the agent first runs and then queries for configuration changes. The default schedule for configuration checks is set to 6:30 AM agent local time every day for endpoint devices and every hour for XenApp servers. Agents running on virtual desktops in a pooled environment will perform configuration checks based on actual usage.

Care should be taken when changing agent properties. These parameters control the way the agent works and could result in users perceiving data loss or an increased CPU usage by the agent. In most cases, you will not need to customize agent properties. Use the default configuration at first and adjust it over time based on user requirements and system performance.

Agent property configurations are displayed on the Agent Properties page (**Company Configuration > Agents > Properties**). When creating a new set of agent properties, you must choose a default configuration (Endpoints Default, XenApp Default, or Virtual Desktop Default) to use as a template. Provide a unique configuration name and description, and edit the parameters as required.

Note: If you have performed an upgrade from an EdgeSight Server version prior to 5.0 SP2, the Virtual Desktop Default configuration is not initially displayed in the list of agent property configurations. To create agent property settings for virtual desktops, select **New Properties Configuration** and then select the **Default Properties for Virtual Desktop Agents** radio button. Configure the properties as described in the “Agent Properties Wizard” topic in online help.

Once a custom set of agent properties has been created, it must be explicitly mapped to a department before it is provided to agents as part of a configuration check. (See “Managing Departments” in [Managing Departments, Devices, and Groups](#) for information on associating a set of agent properties with a department.)

For information on the individual parameters that make up agent properties, see the “Agent Properties Wizard” topic in online help.

Minimal Data Collection Mode

In order to support busy XenApp server environments, the EdgeSight agent has a Minimal Data Collection Mode feature that, when enabled, limits the data collected on the agent and thus the overall impact the agent has on the XenApp server.

When a XenApp server is consistently experiencing heavy load, or the XenApp server slows considerably under load, it is time to consider using this feature. Use EdgeSight reports to note the number of sessions and processes at which a considerable slow down occurs. These numbers are used to establish when Minimal Data Collection Mode is initiated on the agent.

Note: Minimal Data Collection Mode should be considered a temporary measure to ensure that critical data is collected while long term measures are taken to reduce or redistribute the load on the affected XenApp servers.

The Minimal Data Collection Mode is disabled by default. To enable it, edit the agent properties and display the advanced settings. Set **Manage Data Collection** to True and enter values that you collected in the **Process Count Threshold** and **Session Count Threshold** fields. Then assign this set of agent properties to the XenApp server experiencing the problem.

When Minimal Data Collection Mode is enabled, the agent periodically monitors the process and session counts against the configured thresholds. If either threshold exceeds its specified value, the agent enters Minimal Data Collection Mode. At this point an operational alert is sent to the server, “The Citrix System Monitoring Agent has entered Minimal Data Collection Mode.” When both process and session counts return below the threshold settings for 5 minutes, the agent will leave Minimal Data Collection Mode and normal data collection will be resumed. A bullet is sent to the server to indicate that the agent has left Minimal Data Collection Mode.

Minimal Data Collection differs from normal data collection in the following ways:

- No module data is collected or persisted
- No network data is collected or persisted
- No light trace events are persisted
- No image or principal events are persisted (currently not visible)
- No task details used in fault reports will be persisted
- Hung application detection is disabled
- Image and session performance data is persisted at a 2 minute granularity
- Custom performance counter collection is disabled
- Performance, network, and event trace alerts are disabled

Other configuration changes that exist on EdgeSight for XenApp include:

- System, image, and session performance fine grain data is persisted at 15 second intervals.

If the scheduler detects more than 5 concurrent sessions running, it will not use idleness to gate when scheduled items such as consolidation can run. Instead the assumption is made that this is a server system and therefore there may never be best idle moments for schedules to run.

Individual workers can be configured on the server to similarly ignore idleness when making a determination for a best time to run.

Configuring, Scheduling, and Running Workers

Workers are tasks that run on EdgeSight Agents. Default worker configurations and schedules are created during EdgeSight Server installation. You cannot edit or delete default configurations and schedules, but you can use them as templates using the Copy operation and then editing the parameters as required.

Although workers are scheduled to run at certain times, the actual execution of workers takes into account when a user is actively using the system. If possible, workers are run when the system is idle. See “Configuring Workers” later in this topic for more information scheduling workers.

As with agents configurations, care should be taken when changing worker configuration parameters. These parameters control when and how often workers are run and could result in users perceiving increased CPU usage by the agent. In most cases, you will not need to create custom worker configurations. Use the default configuration at first and adjust it over time based on user requirements and system performance.

Once a custom worker configuration has been created, it must be explicitly mapped to a department before it is provided to agents as part of a configuration check. (See “Managing Departments” in [Managing Departments, Devices, and Groups](#) for information on associating worker configurations with departments.)

The EdgeSight workers that you can configure are as follows:

- **Asset History**—Collects the asset history for managed devices. This worker can be disabled.
- **Configuration Check**—Checks for configuration changes to be downloaded to managed devices from the server.
- **Database Maintenance**—Performs database maintenance tasks on the agent database.
- **Drive Space Calculation**—Calculates the drive space used on managed devices. This worker can be disabled.
- **Fault Report Cleanup**—Maintains and cleans up files created for fault and snapshot reports.
- **Performance Upload**—Uploads agent data to the EdgeSight Server.

Configuring Workers

A worker configuration has the following components:

- A configuration name and description—The name and description should be complete enough to allow administrators to accurately select a configuration.

- A set of enabled workers—Only the Asset History and Drive Space Calculation workers can be disabled. All other workers are required to run for proper system operation.
- A set of run conditions—In addition to the worker schedule, a set of run conditions is used to control the behavior of the worker.
- One or more schedules—Each enabled worker must have at least one schedule configured that, along with the run conditions, determines when the worker is run.

The run conditions for workers are as follows. Not all run conditions are set for each worker.

- **Days before the worker will force itself to run**—This setting indicates that the worker will run after the specified number of days, even if other conditions (such as user idle time) are not met. If the worker can not run due to communications problems, it will run as soon as communications are restored.
- **Randomize the start with a window of**—To facilitate system and network performance, worker execution times can be randomized within a time window. This prevents situations such as a large number of agents attempting to upload performance data at the same time.
- **Consider system idle after all users are idle for**—This setting helps to run workers when users are not actively using systems. (The worker schedule has a similar option called **Wait until all users are idle before starting the worker**.)

Note that a run condition must contain a non-zero value to be enabled. Entering zero as the value for a run condition automatically disables that condition. For more information on configuring workers, see the “Workers Configuration Wizard” topic in online help.

Monitoring Workers

Some workers log information into log files. The SYS_EVENT_TXT.txt file indicates which workers have run and at what time. It is located by default in your installation path:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data` for Microsoft Vista and Windows 2008 systems

`%ALLUSERSPROFILE%\Application Data\Citrix\System Monitoring\Data` for all other systems

For agents running on virtual desktops in a pool, the log files are copied to an agent data file share specified during agent installation.

It also logs any errors that may occur when a specific worker tries to run, which is helpful when diagnosing issues. Not all workers create a log file, however, because they are internal to the product and provide product maintenance. The following lists group the workers by the type of task they perform:

Workers that interact with the server:

- worker 101: Performance Upload—uploads Agent data to the EdgeSight server

- worker 104: Init Worker—runs on the initial database creation, connects to the server, and downloads initial agent property information
- worker 105: Configuration Check—checks for configuration changes
- worker 109: Trace Route Worker—executes a network trace
- worker 150: Bullet Worker—uploads alert information to the EdgeSight Server

Workers that collect data:

- worker 102: Drive Space Calculation—calculates drive space on the device
- worker 103: Asset History—collects the asset history of the device

Workers that maintain the agent:

- worker 1: Database Tuning—internal maintenance, no log is created
- worker 2: Database maintenance—internal maintenance, no log is created
- worker 106: AD Worker—runs an Active Directory script
- worker 107: Fault Report Cleanup—maintains and cleans up files created for fault and snapshot reports
- worker 108: Fault Report Preparation—builds fault reports and uploads them to the server
- worker 110: RISH Log Cleanup—maintains and cleans up logs created from RISH
- worker 126: Database Sizing—database size tuning

You may also see other logs different than the ones described above in this directory. This is because some alerts run as scripts and log their activities.

The worker log files contain information that can be useful in troubleshooting issues that can occur relating to the various work functions performed by the agent. You would first look in the `SYS_EVENT_TXT.txt` file to see if a worker has experienced any issues. Based on the information there, you would then look to the specific worker log for more detailed information.

For example, if the `SYS_EVENT_TXT.txt` file makes a reference to the following error message:

```
Running worker 101 - 'Performance Upload' with trigger 1071
```

Then you would look in the log folder for the text file that begins with `Worker101_Trigger1071`.

The most useful logs tend to be the ones associated with the upload and configuration workers, as they help to resolve connectivity issues between the agent and server. For that reason, the logs for workers 101, 104, and 105 are typically the most useful in troubleshooting these sorts of problems. For example, you can verify that agent communication with the server is failing if you examine the `SYS_EVENT_TXT` file, locate Worker 104 running with trigger 24 and see a status of anything other than 0x0.

License Server Monitoring

EdgeSight software can monitor Citrix License Servers for license usage. All related settings are located on the **Configure** tab under the **License Monitor Configuration** menu item.

License server monitoring does not depend on an EdgeSight Agent to gather information. Once a license server has been configured for monitoring, EdgeSight Server directly polls the license server for information on license usage. Polling is performed by the `core_lsm_license_poller` server script. The data returned from the license servers is displayed in the Citrix Licensing reports available from the **Track Usage** tab.

Managing License Server Polling

Use the Settings page to configure how often the specified license servers will be polled and if email is to be sent to the EdgeSight Administrator if polling fails. The timer controlling when polling occurs starts after the previous polling cycle is completed. For example, setting the polling interval to 15 minutes means that a polling cycle will be initiated 15 minutes from the time that the last polling cycle completed. To assist you in selecting a reasonable poll interval, the total time taken to poll all configured license servers is displayed.

As you add more license servers, or network traffic increases, you may need to increase the poll interval to ensure that all servers are polled within the polling interval. Similarly, if you decrease the number of license servers, you may want to reduce the polling interval and retrieve license data more often.

The order in which license servers are polled can change from one polling cycle to the next, because EdgeSight starts by polling the license server which has not been polled for the greatest amount of time. For more information on polling settings, see the “Add or Edit License Server Configuration” topic in online help.

Configuring License Servers for Monitoring

The License Servers page allows you to configure which license servers are to be monitored, enable and disable polling for a server, and delete a server configuration. Once you configure a server and enable polling, the license server is polled in the upcoming polling cycle.

You may want to disable polling for a server if polling errors are occurring and the problem is being investigated, or if the server is being taken down for upgrade or maintenance. Previously collected license information from disabled servers will still appear in the License Usage Trending report, but no new license information is displayed for the disabled server in the License Usage Summary report.

Important: Deleting a license server configuration deletes all license usage data associated with that license server from the EdgeSight database. After deletion, no data from the license server is displayed in the license usage reports.

For more information on configuring license server monitoring see the “License Servers” and “Add License Server Configuration” topics in online help.

Managing Server Settings

Server settings allow you to manage global settings on a Citrix EdgeSight Server. All server settings are located on the **Configure** tab under Server Configuration and Server Status. Server settings allow you to perform the following tasks:

- Monitoring Server Status
- Configuring Server Settings
- Creating Companies
- Configuring Data Uploading
- Managing Licenses
- Managing Authentication Providers
- Configuring the Connection to Reporting Services
- Managing Reporting Services Schedules
- Managing the Database
- Handling Unmanaged Devices
- Displaying Agent Database Broker Status
- Displaying and Responding to Server Messages
- Managing Server Scripts

Monitoring Server Status

The Status page (**Server Configuration > Status**) provides you with an overview of server operations across all companies. The Company table lists how many devices have and have not uploaded data to the server during the current day, by company. It also lists how many new devices running EdgeSight Agent have registered with the server for the current day and during the previous week. The status for messages, unmanaged devices, alerts, and crash reports simply provide a count indicating activity for the current day.

Status Type	For detailed information...
Company	Navigate to Company Configuration > Device Management > Devices to display details on when specific devices uploaded data to the server and to display information on new devices.
Server Script Host	Click Server Script Host Status to display the Server Script Host Status page. Navigate to Server Configuration > Settings and select the applicable tab to display and manage settings for Data Upload and Crash Processing.
Message Status	Click Message Status to display the most recent messages.
Unmanaged Devices	Click Unmanaged Devices to display information on unmanaged devices. An unmanaged device is a system with an EdgeSight Agent installed that is not associated with a company and department.
Alerts	Select the Monitor tab and then select either Alert Console or Alert List to display information about the most recent alert notifications.
Crash Reports	Select the Monitor tab and then select Alert List and filter for Process fault or Process snapshot alerts. See the <i>Citrix EdgeSight User's Guide</i> for more information on accessing and using crash reports.

Configuring Server Settings

The Settings page (**Company Configuration > Settings**) allows you to control how EdgeSight Server handles the following capabilities:

- Agent Support and License Server
- Agent Database Broker Logging
- Notifications
- Timeouts
- Data Uploading
- Application Crash Processing
- SSL Support
- SNMP Port

In most cases, you will not need to adjust any of the values or settings on this page. We recommend that you use the default settings and observe server performance in production conditions before considering the adjustment of server settings.

Agent Support and License Server

Depending on the Citrix EdgeSight products installed in your environment, you may want to enable or disable the display of reports displaying data from XenApp servers or from endpoints. You may also want to select the level of support offered for EdgeSight for XenApp agents: Basic or Advanced.

- *Basic* agents require only that you have a XenApp Enterprise license available on your Citrix Licensing Server. The agent records information about client and server performance and application usage.
- *Advanced* agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix Licensing Server. The agent records information about user sessions, client and server performance, application usage, and network connections.

This setting only determines whether reports and administrative pages are displayed on the console; data continues to be collected, uploaded, and stored even if display support is disabled. Note that unlike alert suppression settings, this is a server wide setting and affects what all users see when using the console. For more information on what tools and reports are displayed based on agent type, see [EdgeSight Feature Availability](#).

To enable or disable support, choose an option from the support drop-down menus. If you select an option which excludes available data from being displayed, such as disabling

XenApp agent support for a server which has EdgeSight for XenApp agents reporting up to it, a confirmation box is displayed.

If EdgeSight for Endpoints support is enabled, you can also edit the name and port of the Citrix License Server which supplies licenses for endpoint systems.

Agent Database Broker Logging

This **Agent Database Broker** tab allows you to enable the display of detailed broker log messages. This option is set to Off by default. If this option is enabled, additional status messages are displayed on the Broker History page. (See “Displaying Broker History” under [Displaying Agent Database Broker Status](#) for more information.) Detailed logging always occurs on the agent database broker; this feature simply controls the display of data on the Broker History page. This feature is useful for providing detailed information when debugging agent database broker issues.

Notifications

The SMTP server name and email addresses are specified during server installation, but can be changed as required.

Important: It is critical to server operation that a valid SMTP server name is used. EdgeSight Server uses the SMTP server for many features, including the distribution of alert notifications, server error conditions, and new user passwords.

The following table defines the notification options. The email options enable the server to send email to the EdgeSight Administrator Email Address in the event of agent or server errors.

Option	Definition
New Agents	This option is recommended as an effective means of notifying an administrator by email that new devices will be uploading data to the server. Client registration is controlled by company-specific settings as described in Managing Company Properties .
Agent Errors	You may want to enable this option when first using Citrix EdgeSight Server to help detect and resolve agent property issues. This option may not be necessary once these issues have been resolved. In most cases, agents are able to automatically recover from errors.
Server Errors	You may want to enable this option when first using Citrix EdgeSight Server to help detect and resolve configuration issues. This option may not be necessary once these issues have been resolved.
Communication Errors	This option is recommended as an effective means of alerting an administrator to device communications problems.
Send an email when there is bad HTTP read of a payload (not recommended)	This option is not recommended for normal use because uploading of payloads is retried as required. You may want to enable this option for use in debugging a specific problem uploading payloads.

Attach Payload	This option is not recommended for normal use because uploading of payloads is retried as required. This option may not be necessary once these issues have been resolved.
----------------	--

Timeouts

Timeouts are specified for common server operations (such as database queries and ASP page loading, data upload queries, and background service queries) to prevent the server from being blocked while waiting for a response to a query. We recommend that you use the default values unless a specific problem occurs with excessive timeouts.

Note that the Farm Monitor and Alert Console (located on the **Monitor** Tab) use the ASP.NET Page and Query timeout when performing queries for alert data. If you experience frequent timeouts when using these pages, increase the ASP.NET Page and Query timeout as required.

Data Uploading

Data uploading refers to the collection of queued database payloads from machines running an EdgeSight Agent. In most cases, the default values are sufficient for proper operation. Values may need to be adjusted if you receive repeated messages warning of too many queued payloads or other data upload issues. Note that the minimum CPU, memory, and active time timeouts are intended to ensure that only data from machines with more than a minimal amount of activity is uploaded to the server. This provides an accurate view of availability and performance data across the company.

Application Crash Processing

Because application crash logs can be large files, the capability is provided to limit the retention of crash logs by number, by disk consumption, and by date. These limits help prevent crash logs from consuming too much space on the server. You can also disable application crash processing, in which case, no crash log files are uploaded to the server.

If either the maximum number of crash logs or the maximum disk consumption limit is exceeded, application crash processing is automatically disabled until the limit is increased. There is no reset operation that can be used to remove existing payloads.

SSL Support

The SSL Support feature enables secure logins. A valid SSL certificate issued by a trusted certificate authority must be present on the server running the EdgeSight Website. If SSL support is enabled, all agent to server communications must be over SSL. If an agent attempts to connect to an SSL-enabled server without using SSL, an error is generated. Any attempts to establish a connection to the agent (such as running a worker remotely or displaying a real time report) will display an error stating that SSL is required, but this connection did not occur over SSL.

SNMP

The SNMP Trap Port to be used for outgoing SNMP trap alert actions. This port setting is used for all SNMP trap alert actions defined for all companies hosted on the server. EdgeSight allows you to set the port so that you can avoid conflicts with other management tools which may be using the default SNMP outgoing port. For more information on creating SNMP trap alert actions, see [Creating Alert Rules and Actions](#).

Creating Companies

A company is the primary organizational unit on an EdgeSight Server. A single server can support multiple companies. You create an initial company when installing EdgeSight Server. After installation and post-installation configuration is complete, navigate to **Server Configuration > Companies** to create additional companies as required.

The only information required for creating a company is a name and a time zone. Company names must be unique on the server. If you have multiple EdgeSight Servers and intend to create reports across servers, ensure that the company name is unique on all the servers.

The time zone is used by the server when displaying time stamps and triggering jobs. There is a single time zone for each company defined on an EdgeSight Server. All data for that company is aggregated based on the day boundary for that time zone. This ensures data consistency when agent machines are in a number of different time zones.

Managing Licenses

This section describes how to manage EdgeSight licenses. For information on configuring EdgeSight to monitor Citrix License Servers, see [License Server Monitoring](#).

Citrix License Server for Windows is used to supply licenses authorizing EdgeSight Agents to upload data to an EdgeSight Server. The license server can be anywhere on the network as long as it can be reached from the EdgeSight Web server and by EdgeSight for XenApp agents. A single license server can be shared by multiple Citrix products, including multiple EdgeSight Servers. It is highly recommended that the license server and EdgeSight for Endpoints license files be in place before completing the initial configuration of EdgeSight.

Important: You must obtain separate licenses for EdgeSight for XenApp and EdgeSight for Endpoints agents, even if both types of agents are associated with the same server.

The EdgeSight for Endpoint agent license file (for example, CESEP_*.lic) is located in the MyFiles folder of the license server directory, for example:
%ProgramFiles%\Citrix\Licensing\MyFiles.

Configuring Licensing for EdgeSight for Endpoints Agents

If EdgeSight for Endpoints support is enabled, you are required to enter a license server name and port during EdgeSight Server installation. During initial configuration using the Post-Installation Wizard, you can test the connection to the license server and, if successful, display the type and number of licenses installed.

EdgeSight Server obtains licenses on behalf of EdgeSight for Endpoints agents from the specified server. You can change the license server name and port after installation by navigating to **Server Configuration > Settings** and editing the **License Server Name** and **License Server Port** fields as described in “Agent Support and License Server” in [Configuring Server Settings](#). The current license server name and port are displayed on the Licensing page, as described in “Using the Licensing Page to Monitor License Status” later in this topic.

Configuring Licensing for EdgeSight for XenApp Agents

After EdgeSight for XenApp Agents are installed, they receive default agent properties from the associated EdgeSight Server. These properties instruct the agent which license server should be contacted to obtain a license. The following license server options are available:

- XenApp—Use the same license server as the XenApp server on which the agent resides. This is the default setting in the XenApp Default agent properties.
- Farm—Use the XenApp Farm’s license server.

- Custom—Use an explicitly defined license server and port.

For more information on agent properties, see [Setting Agent Properties](#) and the “Agent Properties Wizard” topic in online help. As with any agent properties, these settings apply to entire departments and are inherited by sub-departments unless overridden at a lower department level.

EdgeSight for Endpoint Agent Licensing

For EdgeSight for Endpoint Agents, licensing works as follows:

- During post-install configuration, you can validate the connection from the EdgeSight Server to the license server. This is optional, and the post-installation wizard can complete without a valid license or connection.
- The license file installed on the license server specifies the number of EdgeSight for Endpoints agents allowed to upload data to the server.
- EdgeSight Server regularly contacts the license server to determine if sufficient licenses are available. If the license server detects that only a few EdgeSight for Endpoints licenses remain, a warning message is sent to the EdgeSight Server.
- If the number of agents specified in the license is exceeded, agents are not allowed to upload data to the server. Data collection continues and data is retained in the agent database until groomed.

The EdgeSight Server requires one license for each endpoint device reporting up to it. At server startup, the EdgeSight Server attempts to check out one license for each existing device. If not enough licenses are available for the existing devices, all available licenses are checked out and allocated to agents based on when the agent first uploaded data to the server; older agents are given licensing preference over newer agents. Only licensed agents are allowed to upload data to the server. (Devices running agents are tagged as licensed or not licensed in the EdgeSight database.) The server retries license checkouts every minute when it is unable to acquire licenses for all agents. A warning message is added to the messages table and an email is sent to the server administrator. To remedy a shortage of licenses, you must install new licenses, or delete existing devices until compliance is reached.

Once the server is able to properly start up, when a new device reports up to the server, the server checks out a license for that device. After the server has secured a license for a given device, that device can always upload, and further license checks are not performed (except for the startup case mentioned above). If a new endpoint agent is unable to upload due to a license shortage, data collection continues and data is retained in the agent database until groomed. As with the startup case, you must install new licenses, or delete existing devices until compliance is reached before the new devices can upload data.

When a device is deleted from a server, the license for that device is checked in to the license server and available for use by another device.

“Server startup” actually refers to the Server Script Handler (RSSH) startup. When RSSH is stopped, all licenses checked out for that server are checked-in, and available for use by other servers using the same license server, until RSSH restarts. This is important to remember when planning for the number of licenses required. If you have an insufficient number of licenses to cover all devices across all servers, another EdgeSight Server could

check out licenses causing a license shortage at startup.

EdgeSight for XenApp Agent Licensing

For EdgeSight for XenApp Agents, licensing works as follows:

- EdgeSight for XenApp Agents communicate directly with the license server to obtain a license for each session. Agents checkout a license as part of session start on the XenApp server
- If a license is not available, a breach is logged (notifying EdgeSight Server of a problem), but data collection continues for the session. If a user starts more than one session on a XenApp server, or sessions across servers, the same license is used across sessions (as with XenApp licenses).
- The number of license violations is allowed to exceed the value specified in the license, but excess uploads are blocked after 5 days of license violations occur during the license monitoring period. (Multiple license overages on a single day count as a single violation). Excess uploads are blocked and discarded until no more breaches occur for a specified time period or the license is upgraded.
- To help ease installation and configuration, the initial data upload from a XenApp server is not checked for license violation. Any violations in the initial payload are ignored and discarded.

Important: An EdgeSight for XenApp Agent will attempt to monitor all sessions on that XenApp server and cannot monitor only a portion of sessions on the system. In other words, if you purchase EdgeSight for XenApp for a portion of your concurrent user (CCU) base, you need to understand the approximate session load on a given server and then determine how many servers must have the agent deployed to handle the load. Take this information into account when determining license requirements.

Using the Licensing Page to Monitor License Status

Use the Licensing page (**Server Configuration > EdgeSight Licensing**) to display current license usage and status information. The Licensing page displays the following information:

EdgeSight for XenApp License Statistics

<p>Current Licensing Status</p>	<p>Indicates whether the system is in compliance with the license. In compliance indicates that the number of allowed license violation days have not been exceeded. The license status can be one of the following:</p> <p>In Compliance—All of the existing devices reporting to this server were able to acquire licenses.</p> <p>Warning—The number of licenses used has exceeded the number of licenses allowed during this monitoring period. See the Violation Days field for the number of violation days and the servers reporting the violations.</p> <p>In Violation—The number of licenses used has exceeded the number of licenses allowed for at least 5 days during this monitoring period.</p>
<p>New Device Grace Period</p>	<p>During this period, agents reporting up with licence violations will not have payloads rejected. A warning email is sent to the EdgeSight Administrator, and a message is posted to the Messages page, indicating that a license violation has occurred. This feature allows administrators to fix problems with initial configurations.</p>
<p>Allowed Violation Days</p>	<p>The number of days during the monitoring period for which the number of licenses used are allowed to exceed the number of licenses granted. Uploads are blocked if the number of violation days in the monitored period exceeds five (5) days.</p>
<p>Violation Monitoring Period</p>	<p>The number of days for which license violations are tracked.</p>
<p>Violation Days</p>	<p>The current number of days during the monitoring period for which the number of licenses exceeded the number of licenses granted. Expand this item to display the dates of license violation and the names of the servers reporting the violation.</p>
<p>Endpoint License Statistics</p>	

<p>Current Licensing Status</p>	<p>Indicates whether the system is in compliance with the license. The license status can be one of the following:</p> <p>In Compliance—The EdgeSight Server was able to acquire licenses for all of the existing devices reporting to this server.</p> <p>Error—The EdgeSight Server was unable to acquire licenses for all of the existing devices on this server. EdgeSight will continually attempt to acquire licenses for all devices.</p> <p>Stopped—The License Manager is not currently running.</p> <p>You may also see a message informing you that the server is in the process of acquiring licenses. If, on startup, the server is unable to acquire licenses for all registered endpoint devices, a message is displayed and the server retires license acquisition every 15 minutes. You can retry immediately by clicking the Refresh Endpoint Licensing button. This button is only displayed if there is a license acquisition failure on startup.</p>
<p>Licensed Devices on This Server</p>	<p>The number of endpoint licenses currently in use by agents reporting to this server. This is displayed in terms of the total number of agents registered with the server. For example, if there are 500 agents registered with the server, and 487 agents are currently using licenses, this field would display 487 of 500.</p>
<p>License Server</p>	<p>The license server name and port number from which EdgeSight obtains endpoint agent licenses. The server and port are specified during installation and can be changed after installation on the Settings page.</p>
<p>Total Installed Licenses</p>	<p>The total number of endpoint agent licenses specified by the installed license file.</p>
<p>Available Licenses</p>	<p>The number of licenses available for use by endpoint agents.</p>
<p>Expiration Date</p>	<p>The date at which the license file will expire. You will be notified prior to license file expiration.</p>

Managing Authentication Providers

Authentication providers ensure that only authorized users can log on to an EdgeSight Server. The first step in creating a new user is to select an authentication provider against which a username and password are verified.

A default authentication provider (Email) is included when you install EdgeSight Server. You cannot edit or delete the default authentication provider. The default authentication provider uses an email address as the username. When you create a new user, you specify the email address for the user. Then, an email is sent to the user explaining the sign in process and providing a temporary password. When the user first logs on, they are requested to change their password.

You can create new authentication providers that use Active Directory (AD) for security and sign-on capabilities. Before creating a new provider, make sure you have the LDAP path for your AD authentication provider available.

To set up Active Directory integration with EdgeSight, you must set up an Active Directory authentication provider: Before you begin, make sure you have the LDAP path for your authentication provider available.

1. Log into the EdgeSight Server Console.
2. Navigate to **Server Configuration > Authentication** in the navigation pane to display the Authentication Configuration page. Note that the Email provider is already listed.
3. Click the **New Provider** button to invoke the Authentication Provider Wizard.
4. Click **Help** and follow the instructions provided in the Authentication Provider Wizard topic.

Setting Up Users and/or Groups

Once you have added an authentication provider and set up roles, you must also set up users and/or groups. You may want to create multiple groups within your Active Directory, such as an EdgeSight Admin Group, and an EdgeSight Console User Group for ease of Administration.

1. Navigate to **Company Configuration > Security > Users** in the navigation pane to display the Manage Users page.
2. Click the **New User** button to display the User wizard.
3. Click **Help** and follow the instructions provided in the Add User Wizard topic.
4. Test the new user or group setup. Log out of the EdgeSight Server and log in again. At the Login page, the **Provider** drop-down menu is now displayed. The user or group member selects the applicable provider and then logs in using their domain user ID and password.

Configuring Reporting Services

Configuring the Connection to Reporting Services

Microsoft SQL Server Reporting Services must be installed and configured in order to generate and display EdgeSight reports. For detailed installation and configuration procedures for Reporting Services and related software, see *Configuring Reporting Services for Citrix EdgeSight*.

After the Reporting Services installation and configuration is complete, you must configure the connection from EdgeSight Server to the Report Server. Navigate to **Server Configuration > Reporting Services > Report Server** to specify the report server, credentials for accessing the report server and the data source, and default report and schedule operations. For more information, see the “Report Server Settings” topic in online help.

Managing Reporting Services Schedules

Reporting Services schedules, in conjunction with the subscription feature, allow you to automate the generation of reports for distribution to users. When an administrator or a user creates a report subscription, they must select an associated schedule. Navigate to **Server Configuration > Reporting Services > Schedules** to manage existing schedules and create new schedules. For more information, see the “Reporting Services Schedules” topic in online help.

In some cases, such as a week with a holiday or a scheduled company shutdown, you may want to pause report schedules so that the associated reports are not generated.

Care should be taken when deleting schedules. If the deleted schedule is associated with a report, the report will not be generated. Also, subscriptions using the deleted schedule will not result in a report distribution.

Managing the Database

You can manage the size of the EdgeSight database by configuring what data is uploaded from agents to the server and how long data is retained before being groomed. These tasks can help ensure acceptable database performance.

Configuring Data Uploading

You can select what types of performance and availability data you want to upload to the server (**Server Configuration > Data Maintenance > Upload Configuration**). This allows you to optimize EdgeSight Server performance by limiting data uploads to reflect the data used in your enterprise.

The uploading of XenApp Environmental Usage data is disabled by default, and should only be enabled if you plan to use the Environmental Usage report, which displays this data. Depending on the number of sessions for the group or device, the data used to generate these reports can significantly increase the size of your EdgeSight database. In many cases, you may want to enable data collection for a period of time as required and then disable data collection when no longer needed.

Database Grooming

EdgeSight collects a wide range of performance, availability, and usage data about end-user systems, applications, user sessions, and the network. The EdgeSight Agents collect data from systems and upload it to a EdgeSight Server. Depending on the number of endpoint and XenApp systems, the number of applications, and network activity, databases can grow quickly without proper management. The primary database management mechanism is grooming.

Grooming is the process of removing older data from a database at regular intervals to make room for new data. Grooming is critical for maintaining efficient database operation. An effective grooming schedule controls database size and helps ensure acceptable performance while retaining sufficient data for business operations.

The following example shows how database grooming settings affect the size of the EdgeSight Server database. You have deployed EdgeSight agents on 2500 end user devices. The devices are running an average of 50 processes and visit an average of 100 Websites over the period of time that network data is retained. The agents are collecting data for 12 hours each workday. Changing the grooming parameter for Network Statistics from 7 to 14 days increases the size of the database by about 40 percent, roughly equivalent in its effect on database size to adding 1000 devices.

Grooming Schedule

EdgeSight has a distributed structure, with EdgeSight Agent databases on each managed device which are uploaded to a single EdgeSight Server database. The data retention

settings for the agent database are specified as part of the agent properties and are applied to devices based on their department membership. If persistent data upload timeouts occur for agents using the same configuration, you may want to consider decreasing the values for the Days To Keep In DB and Max Days To Keep In DB agent configuration settings. In some cases, this may result in a loss of data, especially if managed devices are unable to connect to the EdgeSight Server.

The grooming schedule for the server database is specified as part of the server configuration. The server grooming schedule allows you to specify the number of days that data is retained by data type. This allows data used to identify trends, such as performance data, to be retained longer than data which quickly becomes stale, such as real-time alert data.

The default values for grooming the server database are sufficient for most installations. You may want to use the default values at first and adjust them over time based on user requirements and system performance. In cases where you want to retain more data, consider creating an archive report or performing data warehousing as methods of keeping historical data in preference to relaxing the grooming configuration. See the *Citrix EdgeSight User's Guide* for more information on using EdgeSight data for analysis and record keeping.

Server Database Grooming

Navigate to **Server Configuration > Data Maintenance > Grooming** to edit the database grooming schedule, as described in the “Grooming Configuration” online help topic. The Grooming table contains the following information:

- Report Data—The type of data to be groomed.
- SQL Server Table—The database table where the data is stored.
- SQL Server View—The SQL views associated with the database table where the data is stored. These views are used in modifying reports and creating custom reports. Online help includes definitions of all views.
- Groom Days—The default number of days that data of the selected type is retained before grooming is performed.

In most cases, the grooming schedule is configured to retain one month of data. Application usage data is retained for 90 days due to the need in many environments to track application usage for license and compliance reporting. On the other hand, network data is only retained for 10 days due to high data volumes and the transient nature of the data.

The grooming strategy for a specific data type should take into account how fast the usefulness of the data decreases from time of collection and also how much data is collected on average over a time period. For example, the data in the alert_incoming table has a short shelf life. Real-time alerts are intended to address critical problems that can be resolved by taking action within a short timeframe, such as crashes of mission-critical applications or disruptive network failures. Because of these characteristics and because historical alert data is retained, real-time alert data is groomed aggressively.

It is important to ensure that the grooming schedule is taken into account if data is being warehoused or reports are being archived. If data is transferred less frequently than the grooming schedule for a type of data, data loss can occur. Similarly, report archiving schedules must take into account the grooming schedule to avoid introducing gaps in

historical reports.

You can monitor the status of grooming jobs by displaying the grooming log (**Server Status > Grooming Log**). The log displays the following information:

- **Data Area**—The type of data on which grooming was performed.
- **Grooming Job Name**—The name of the grooming job run, such as `core_groom_instance`.
- **Job Status**—The completion status of the job, such as “The maintenance job succeeded.”
- **Start Time**—The date and time that the grooming job started.
- **Duration**—The elapsed time taken by the grooming job. Note that in the case of smaller databases, grooming jobs may show a duration of zero time.

Managing Maintenance Jobs

In addition to grooming, there are a number of other maintenance jobs which are performed by an EdgeSight Server. These include dealing with data uploads and clearing caches and temporary storage areas. Each job is associated with a schedule, either Fifteen Minute or Nightly. The Fifteen Minute schedule runs jobs at fifteen minute intervals whenever EdgeSight Server is operational and is not configurable. The Nightly schedule runs jobs once a night and can have a start time configured. By default, the start time is five minutes after midnight based on server time. This allows the job to run to completion when the fewest users are active. The following table shows which console pages to display when managing maintenance jobs.

Console Page	Operations
Server Configuration > Data Maintenance > Jobs	Display job schedules, edit the start time for the Nightly schedule, and manually run jobs associated with schedules.
Server Status > Job Status	Determine when jobs last ran and their completion status. You can also display the overall duration of the set of jobs and the last run duration of individual jobs.
Server Status > Job Log	Display the run history of individual jobs, including result, duration, and start time.

Handling Unmanaged Devices

Unmanaged devices are systems running an EdgeSight agent that are not associated with a company and department. The agent can communicate with the server and be included in the list of unmanaged devices as long as it has a valid server and port specified during installation. Devices may be unmanaged due to the following reasons:

- The Company information provided by the agent when it registered with the server did not match an existing company.
- The Automatically register agents setting is disabled. (For more information, see “Agent Registration Settings” in [Managing Company Properties](#).)
- A database corruption has occurred on the device and recovery has failed.

You can monitor the number of unmanaged devices from the System Status page or by navigating to **Server Settings > Configuration > Unmanaged Devices**. The Unmanaged Devices page allows you to move a device to a company and department. Devices running EdgeSight for XenApp 5.0 agents can only be moved to the PS Farms department. All other devices can be moved to the Endpoints department. For agents that were previously registered with the server, the department to which the device last uploaded data is displayed in the **Registered Org** field.

The EdgeSight Agent on an unmanaged device collects data and uploads data to the server but will not appear in any historical or real-time reports. The data is subject to grooming, so allowing devices to remain unmanaged for lengths of time may result in lost data. Review the **Last Upload** field to determine when the agent on the device last communicated with the server.

Displaying Agent Database Broker Status

The configuration pages under the Agent Database Broker folder (Pools, Agent Database Servers, and Broker History) only display data if the EdgeSight Server is acting as a database broker for EdgeSight for Endpoints Agents installed on virtual desktops in a pooled environment. Although the database broker components are included in all EdgeSight Server installations, they are not used unless the server is specified as the database broker during the Agent Database Server and the EdgeSight Agent installations. For a description of the various components required for monitoring virtual desktops, see [Installing EdgeSight for Monitoring Virtual Desktops](#).

These pages reflect the status reported by Agent Database Servers, pools, and devices (in this case, virtual desktops running EdgeSight agents). In most cases, actions taken on these pages are housekeeping changes, such as deleting an unused pool or deleting stranded registration information for an Agent Database Server. Actions which directly affect your environment are rebalancing pools and enabling/disabling Agent Database Servers.

Displaying Pool Status and Rebalancing Pools

Use the Pools page (**Configuration > Server Configuration > Agent Database Broker > Pools**) to display information about pools (named groups of virtual desktops). The pool name corresponds to the XenDesktop desktop group name. In addition to displaying pool status, you can rebalance or delete pools.

The rebalance feature allows you to manually force a redistribution of agents in relation to database servers. The agents are not immediately rebalanced; the redistribution takes place over time as virtual desktops are shut down and rebooted.

Caution: Rebalancing agents in a pool across the database servers results in the loss of EdgeSight Agent data stored on those servers. Do not perform a manual rebalancing if you need to preserve agent data.

Deleting pools is a housekeeping function that should be performed when all the agent database servers associated with a pool have been deleted. For more information about pool rebalancing and deletion, see the “Pools” topic in online help.

Displaying Database Server Status

Use the Agent Database Servers page (**Configuration > Server Configuration > Agent Database Broker > Agent Database Servers**) to display current server status and to perform actions related to all the agent database servers which have registered with the database broker components of EdgeSight Server. You can disable/enable and delete servers.

If maintenance is required or a problem has occurred on a database server, you can disable the database server. Disabling a server means that the database broker components of EdgeSight Server do not broker the server to new agents. The agents already using the database server continue to store data in the database. Once the maintenance has been performed or the issue resolved, you can enable the server to make it available for

brokering to agents.

Deleting an agent database server only deletes the registration data stored on the EdgeSight Server database, such as the agent database server name, port, and pool association. The feature is designed to allow you to remove a stranded registration for a server which has been uninstalled or assigned to another EdgeSight Server.

For more information on server status, disabling/enabling servers, and deleting servers, see the “Agent Database Servers” topic in online help.

Displaying Broker History

Use the Broker History page (**Configuration > Server Configuration > Agent Database Broker > Broker History**) to display status messages for EdgeSight Agent Database Servers, pools, and devices. The message list can be filtered by server, pool, or device, providing a chronological history of the selected component. Most messages are informational, but errors are displayed for agents which are unable to connect to a database server. Note that long error strings are truncated to about 512 characters. See the “Broker History” online help topic for more information on individual columns in the Broker History table.

Troubleshooting Database Broker Issues

You can enable detailed logging for use in debugging broker issues on the **Agent Database Broker** tab at **Server Configuration > Settings**, as described in “Agent Database Broker Logging” in [Configuring Server Settings](#).

During installation, an agent can be configured to contact the EdgeSight Server acting as a database broker to receive a database connection string. If the fails to get a database connection, the agent shuts down and writes error information to the local SYS_EVENT_TXT.TXT log. If the File Monitor service on the agent is functioning properly, a copy of this file will be copied to the agent data file share. If the problem is that an incorrect path was supplied for the database broker, you can change configuration settings using the Citrix System Monitoring Agent control panel applet. However, you must make those changes on the base image in order for them to be propagated to all desktops. For more information on installing and configuring agents in a pooled environment, see [Installing EdgeSight for Monitoring Virtual Desktops](#).

Displaying and Responding to Server Messages

The Messages page (**Server Status > Messages**) displays status and event messages for EdgeSight Server and for devices running EdgeSight Agents. You can filter the list of messages by message type (All Types, Error, Warning, Informational, New Device, or Active Monitoring) and by company (All Companies, No Company Specified, or a specific company).

Managing Server Scripts

The Server Script Host page (**Server Status > Server Script Host**) displays the status of services on EdgeSight Server. These services include basic server functions, such as alert, payload and crash file handling, and maintenance functions, such as the cleanup of temp folders and crash report folders. Each service has an associated log file which may be helpful in isolating problems with server operations. You can also start and stop services, although this should generally be done at the direction of Citrix Technical Support.

EdgeSight Feature Availability

The data collected and displayed depends on the type and version of EdgeSight Agent installed and the version of the XenApp server or Presentation Server being monitored. Feature availability information can be broken down as follows:

- by agent type
- by agent version
- by XenApp or Presentation Server version

EdgeSight Feature Availability By Agent Type

This section provides information about what features will be displayed and data collected based on the Agent Support settings (**Configure tab > Server Configuration > Settings**). The server features are broken out by the tab on which they appear in the EdgeSight Server Console or by feature type, such as alerts. An X indicates that the feature or data is present. If the column is blank, the feature or data is not present.

Note: The agent support settings only control the display of data on the console; they do not affect the collection of data by agents.

EdgeSight provides the following types of agents:

- **EdgeSight for Endpoints** – Endpoint agents provide monitoring and data collection for endpoint devices.
- **EdgeSight for Virtual Desktops Agent** – Virtual desktop agents monitor virtual desktops based on XenDesktop 4.0. In addition to monitoring system, application, and network performance, it collects ICA channel data including XenDesktop multi-media counters, collects end user experience metrics, and alerts on XenDesktop session performance. Note that this agent does not provide monitoring of the Desktop Delivery Controller (DDC).
- **EdgeSight for XenApp, Basic** – Basic agents require only that you have a XenApp Enterprise license available on your Citrix License Server.
- **EdgeSight for XenApp, Advanced** – Advanced agents provide the fully featured version of EdgeSight for XenApp and require that you have either a XenApp-Platinum Edition license or an EdgeSight for XenApp license available on your Citrix License Server.

Monitor Tab

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Alert Console	X	X	X	X
Dashboard	X	X	X	X
Alert List	X	X	X	X
Farm Monitor		X	X	X

Troubleshoot Tab

The following features are available on the **Troubleshoot** menu:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Device Troubleshooter	X	X	X	X
Device Process List	X	X	X	X
Find EdgeSight Servers	X	X	X	X
Device Trace Route	X		X	X
User Troubleshooter		X	X	

The following features are available on the **Real-time Reports** menu:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Device Summary	X	X	X	X
Alert List	X	X	X	X
System Performance	X	X	X	X
System Compare	X	X	X	X
Custom Performance Counters	X	X	X	X
Network Performance	X		X	X
XenApp Summary		X	X	
XenApp User Summary			X	

Plan and Manage Tab

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Overview	X	X	X	X
Device Summary	X	X	X	X
Process Performance Summary by Process	X	X	X	X

EdgeSight Feature Availability By Agent Type

Process Summary	X	X	X	X
Network Summary	X		X	X
Network Summary by Site	X		X	X
Network Transaction Summary	X		X	X
Process Stability Summary by Process	X		X	X
XenApp Summary		X	X	
User Summary for a User Group			X	X
XenApp User Summary			X	
XenDesktop Summary				X
XenDesktop User Summary				X

Track Usage Tab

Note: Citrix Licensing reports are not dependent on EdgeSight Agents and are therefore not affected by agent support settings.

The following **Published Applications** features are available:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Launch Summary for a Farm			X	
Launch Summary for a User Group			X	
Summary for a Farm			X	
Summary for a User Group			X	
Users Summary for a Farm			X	
Users Summary for a User Group			X	

The following **Session Duration** features are available:

Feature	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Session Duration for a Farm		X	X	X
Session Duration for a User Group		X	X	X

Browse Tab

Note: The License Server Monitor Archive report is not dependent on EdgeSight Agents and is therefore not affected by agent support settings.

The following reports will display data for all agent support settings (Endpoint, XenApp Basic, XenApp Advanced, and Virtual Desktop):

- Alerts
- Asset Changes
- Assets for a Device
- Device Archive
- Device Summary
- Error Archive
- Event Log Alerts
- Event Log Alerts for a User Group
- New Processes
- Process CPU
- Process Cumulative CPU
- Process Memory Usage
- Process Pages Per Second
- Process Performance Archive
- Process Performance Summary by Process
- Process Stability Summary by Process
- Process Summary
- Process Thread Count
- Process Usage
- Process Usage Archive
- Real-time Alert List
- Real-time Device Summary
- Real-time System Compare

- Real-time System Performance
- Software Asset Changes
- System CPU
- System CPU Summary
- System Disk Usage
- System Disk Usage Archive
- System Disk Usage Summary
- System Kernel for a Device
- System Memory Summary
- System Memory Usage
- System Page Faults
- System Performance Archive
- Trace Event Archive

The following reports will display data for the Endpoint, XenApp Basic, and XenApp Advanced agent support settings, but not for the Virtual Desktop support setting:

- Real-time XenApp Summary
- Reboots

The following reports will display data for the Endpoint, XenApp Advanced, and Virtual Desktop agent support settings, but not for the XenApp Basic support setting:

- Hardware Alerts
- Hardware Asset Changes
- Network Connection Archive
- Network Summary
- Network Summary by Site
- Network Transaction Archive
- Network Transaction Summary
- New Sites
- Port Network Delay

- Port Network Round Trip Time
- Port Network Volume
- Port Web Errors
- Process Errors
- Process Errors for a User Group
- Process Faults
- Process Faults for a User Group
- Process Network Delay
- Process Network Volume
- Process Not Responding Alerts
- Process Not Responding Alerts for a User Group
- Real-time Network Performance
- Site Network Delay
- Site Network Errors
- Site Network Round Trip Time
- Site Network Volume
- Transaction Network Delay
- Transaction Network Round Trip Time
- Transaction Network Volume
- Transaction Web Errors
- Visited Sites

The following reports will display data for the XenApp Basic, XenApp Advanced, and Virtual Desktop agent support settings but not for the Endpoint support setting:

- Environmental Usage
- Environmental Usage Archive
- Session Client Type
- Session Duration
- Session Duration for a User Group

- System Memory for a User Group
- User Logon Details
- User Logon Details for a User Group

The Real-time XenApp User Summary report will display data for the Endpoint and XenApp Advanced agent support settings but not for the XenApp Basic and Virtual Desktop agent support settings.

The following reports will display data for the XenApp Basic and XenApp Advanced agent support settings but not for the Endpoint and Virtual Desktop agent support settings:

- Session Counts
- CPU Utilization Management
- IMA Service Availability
- IMA Service State
- Session Login Time
- Session Login Time for a User Group
- XenApp Server Utilization
- XenApp Summary
- XenApp System Performance Archive

The following reports will display data for the XenApp Advanced and Virtual Desktop agent support settings but not for the XenApp Basic and Endpoint agent support settings:

- Session Auto-Reconnects
- Session Client and Server Startup Duration
- Session Client Startup Duration
- Session Client Startup Time Archive
- Session Memory
- Session Network Bandwidth Used
- Session Network Delay
- Session CPU
- Session CPU for a User Group
- Session Network Delay for a User Group

- Session Network Round Trip Time
- Session Network Round Trip Time for a User Group
- Session Network Volume
- Session Network Volume for a User Group
- Session Page Faults
- Session Performance Archive
- Session Server Startup Duration
- Session Server Startup Time Archive
- Session Startup Duration Details
- Site Network Errors for a User Group
- User Logon Counts
- User Summary for a User Group
- ICA Audio I/O
- ICA Client Version
- ICA Drive I/O
- ICA Printer I/O
- ICA Session Compression
- ICA Session I/O
- ICA Session Round Trip Time
- ICA Session Round Trip Time Archive
- ICA Session Round Trip Time for a User Group
- ICA Session Traffic
- ICA Session Traffic for a User Group
- ICA Video I/O

The following reports will display data only for the XenApp Advanced agent support setting but not for the Endpoint, XenApp Basic and Virtual Desktop agent support settings:

- Published Application Launch Archive
- Published Application Launch Count - Details

- Published Application Launch Count for a User Group - Details
- Published Application Launch Summary
- Published Application Launch Summary for a User Group
- Published Application Summary
- Published Application Summary for a User Group
- Published Application User Count - Details
- Published Application User Count for a User Group - Details
- Published Application User Summary
- Published Application User Summary for a User Group
- XenApp User Summary
- Application Response Failures
- Application Response Time
- Application Response Time for a Test
- ICA Session Latency
- ICA Session Latency for a User Group

The following reports will display data only for the Virtual Desktop agent support setting but not for the Endpoint, XenApp Basic and XenApp Advanced agent support settings:

- HDX MediaStream I/O
- HDX Plug-n-Play I/O
- XenDesktop Summary
- XenDesktop User Summary

Alerts

The following alerts are generated for all agent support settings (Endpoint, XenApp Basic, XenApp Advanced, and Virtual Desktop):

- Application Performance
- High Application Resource Usage
- New Process

- System Disk Bottleneck
- System Low Resources
- System Performance
- System Slowdown
- System Thrashing
- Thrashing Application
- Windows Event Log
- Windows Event Log: Application Error
- Windows Event Log: Security Audit Failure
- Windows Event Log: System Error

The Device Reboot alert is generated for the Endpoint, XenApp Basic, and XenApp Advanced agent support settings but not for the Virtual Desktop support setting.

The following alerts are generated for the Endpoint, XenApp Advanced, and Virtual Desktop agent support settings but not for the XenApp Basic support setting:

- Application Error
- Light Trace Event
- Network Connection Performance Exceeded SLA
- Network Socket Error
- Network Transaction Failure
- Network Transaction Performance Exceeded SLA
- Plug and Play Hardware Change
- Process Fault
- Process Hung
- Process Snapshot

The following alerts are generated for the XenApp Basic, XenApp Advanced, and Virtual Desktop agent support settings but not for the Endpoint support setting:

- Print Services Failure
- Session Performance
- Slow ICA Connection

The Physical Disk Failure alert is generated for the Endpoint and XenApp Advanced agent support settings but not for the XenApp Basic and Virtual Desktop support settings.

The following alerts are generated for the XenApp Basic and XenApp Advanced agent support settings but not for the Endpoint and Virtual Desktop agent support settings:

- Active Session Count High
- Client Update Communication Failure
- Client Update Database File Read Failure
- Client Update Database Read Failure
- Client Update Directory Read Failure
- Client Update File Cache Failure
- Client Update File Enumeration Failure
- Client Update ICA File Read Failure
- Client Update Installation Commencement Failure
- Client Update Installation Configuration Read Failure
- Client Update Insufficient Disk Space
- Client Update Insufficient Permissions Error
- Client Update Memory Allocation Failure
- Client Update New Version Send Failure
- Client Update Termination Failure
- Client Update Upgrade Failure
- Configuration Logging Database Unavailable
- Dominant Session
- Excess Disconnected Sessions
- Farm Data Store Connection Failure
- Health Monitoring and Recovery Action Failure
- Health Monitoring and Recovery Test Failure
- IMA Service is Unresponsive
- License Server Connection Failure
- Maximum Farm Connections Exceeded

- Number of Servers in a Zone is Too High
- Published Application Concurrent Usage Limit
- Session Idle too Long
- Session in Down State
- Terminal Server Client Connection Error
- Terminal Server License Server Discovery Failure
- Thrashing Session
- XenApp System Performance
- Zone Data Collector Election Triggered
- Zone Elections too Frequent

The following alerts are generated for the XenApp Advanced agent support setting but not for the Endpoint, XenApp Basic and Virtual Desktop agent support settings:

- Application Response Failure
- Application Response Time
- Session Disconnected
- Session Performance (without EUEM)
- Slow ICA Connection (without EUEM)

The following alerts are generated only for the Virtual Desktop agent support setting but not for the Endpoint, XenApp Basic and XenApp Advanced agent support settings:

- Desktop Registration Failed
- Heartbeat Halted
- VDA Failed to Start

Agent Data Collection

Data Type	Endpoint	XA Basic	XA Advanced	Virtual Desktop
Custom Performance Monitoring	X	X	X	X
Device Asset Changes	X	X	X	X

Disk Usage	X	X	X	X
Light Trace Events	X	X	X	X
Process Performance	X	X	X	X
Process Usage	X	X	X	X
Remote Agent Access	X	X	X	X
System Performance	X	X	X	X
Application Errors	X		X	X
Application Not Responding	X		X	X
Network Performance	X		X	X
Network Transactions	X		X	X
Process Crashes/Snapshots	X		X	X
System Performance		X	X	X
IMA Service State		X	X	
EUEM Data			X	X
ICA Channel Performance			X	X
Print Services			X	X
Session Performance			X	X
Active Application Monitoring			X	

Configure Tab

All Configure tab features are displayed to users with administrative privileges with the following exceptions based on agent support setting:

- If EdgeSight for XenApp support is disabled, the Farm Authentication page is not displayed.
- If EdgeSight for XenApp support is disabled or set to Basic, the IP Ranges page and the EdgeSight Licensing page are not displayed.
- If only EdgeSight for Virtual Desktop agent support is enabled, the EdgeSight Licensing page is not displayed.

Active Application Monitoring Support

The EdgeSight for XenApp Agent running in Advanced Mode is required for the recording of Active Application Monitoring scripts.

EdgeSight Feature Availability By Agent Version

The type of data collected depends on the version of EdgeSight Agent installed on a device. Some reports and SQL views will not return data if the collection of that type of data is not supported by the agent.

EdgeSight 5.2 Agents

The EdgeSight for Virtual Desktops Agent was added for in EdgeSight 5.2. This agent is required for the collection of data displayed in the following reports:

- XenDesktop Summary
- XenDesktop User Summary
- HDX MediaStream I/O
- HDX Plug-n-Play I/O

Either the EdgeSight for XenApp 5.x agent or the EdgeSight for Virtual Desktops 5.2 agent is required for the collection of data displayed in the following new reports:

- ICA Client Version
- User Logon Counts

A number of new SQL views were added in EdgeSight 5.2. See the Virtual Desktop SQL Views topic in the online help for definitions of these views. Note that many of the views are shared by the XenApp and XenDesktop monitoring capabilities of EdgeSight. Views named `vw_vda_*` are only for use in retrieving data from virtual desktops. Views named `vw_xa_vda_*` can be used to retrieve data from either a XenApp server or a virtual desktop. Select the view that matches the types of machines in your environment. Note that EdgeSight does not currently monitor Desktop Delivery Controller (DDC) systems.

EdgeSight for XenApp 6 Agent x64 5.3

EdgeSight for XenApp 6 Agent x64 5.3 (64-bit) is designed to monitor XenApp 6.0 systems. It does not monitor earlier XenApp versions. EdgeSight Server 5.3 includes a new SQL view for published application events (`vw_ctrx_archive_published_app_event`). Note that published application event data is collected by both the EdgeSight 5.2 agents and EdgeSight for XenApp 6 Agent x64 5.3 (64-bit).

Data Collection by Presentation Server or XenApp Server Version

The type of data collected and displayed depends on the version of Presentation Server or XenApp Server being monitored as well as on the version of EdgeSight Agent installed on a device. Some reports and SQL views will not return data if the collection of that type of data is not supported by the version of the server being monitored or by the version of the agent.

Reports

Reports display data based on the version of XenApp or Presentation Server with an EdgeSight 5.2 or later agent. In some cases, the display of data may be limited by the use of older agent versions. For information on the relationship of agent version to data collection, see [EdgeSight Feature Availability By Agent Version](#).

Note: The License Server Monitor Archive report contains data collected by the EdgeSight Server from a Citrix License Server. See the System Requirements topic for your EdgeSight release for more information.

The Session Login Time and Session Login Time for a User Group reports only display information for pre-4.5 XenApp servers without EUEM data and any pre-5.2 agent.

The XenDesktop Summary and XenDesktop User Summary reports contain data on XenDesktop.

The following reports display data for all supported versions of XenApp or Presentation Server (Presentation Server 4.5, XenApp 5.0 or XenApp 5.0 Feature Pack 2, and XenApp 6.0):

- Alerts
- Asset Changes
- Assets for a Device
- CPU Utilization Management
- Device Archive
- Device Summary
- Environmental Usage
- Environmental Usage Archive
- Error Archive

- Event Log Alerts
- Event Log Alerts for a User Group
- Hardware Alerts
- Hardware Asset Changes
- ICA Audio I/O
- ICA Client Version
- ICA Drive I/O
- ICA Printer I/O
- ICA Session Compression
- ICA Session I/O
- ICA Session Round Trip Time
- ICA Session Round Trip Time Archive
- ICA Session Traffic
- ICA Session Traffic for a User Group
- ICA Video I/O
- IMA Service Availability
- IMA Service State
- Network Connection Archive
- Network Summary
- Network Summary by Site
- Network Transaction Archive
- Network Transaction Summary
- New Processes
- New Sites
- Port Network Delay
- Port Network Round Trip Time
- Port Network Volume
- Port Web Errors

- Process CPU
- Process Cumulative CPU
- Process Errors
- Process Errors for a User Group
- Process Faults
- Process Faults for a User Group
- Process Memory Usage
- Process Network Delay
- Process Network Volume
- Process Not Responding Alerts
- Process Not Responding Alerts for a User Group
- Process Pages Per Second
- Process Performance Archive
- Process Performance Summary by Process
- Process Stability Summary by Process
- Process Summary
- Process Thread Count
- Process Usage
- Process Usage Archive
- Published Application Launch Archive
- Published Application Launch Count - Details
- Published Application Launch Count for a User Group - Details
- Published Application Launch Summary
- Published Application Launch Summary for a User Group
- Published Application Summary
- Published Application Summary for a User Group
- Published Application User Count - Details
- Published Application User Count for a User Group - Details

- Published Application User Summary
- Published Application User Summary for a User Group
- Real-time Alert List
- Real-time Device Summary
- Real-time Network Performance
- Real-time System Compare
- Real-time System Performance
- Real-time XenApp Summary
- Real-time XenApp User Summary
- Reboots
- Session Auto-Reconnects
- Session Client and Server Startup Duration
- Session Client Startup Duration
- Session Client Startup Time Archive
- Session Client Type
- Session Counts
- Session CPU
- Session CPU for a User Group
- Session Memory
- Session Network Bandwidth Used
- Session Network Delay
- Session Network Delay for a User Group
- Session Network Round Trip Time
- Session Network Round Trip Time for a User Group
- Session Network Volume
- Session Network Volume for a User Group
- Session Page Faults
- Session Performance Archive

- Session Server Startup Duration
- Session Startup Duration Details
- Site Network Delay
- Site Network Errors
- Site Network Errors for a User Group
- Site Network Round Trip Time
- Site Network Volume
- Software Asset Changes
- System CPU
- System CPU Summary
- System Disk Usage
- System Disk Usage Archive
- System Disk Usage Summary
- System Kernel for a Device
- System Memory for a User Group
- System Memory Summary
- System Memory Usage
- System Page Faults
- System Performance Archive
- Trace Event Archive
- Transaction Network Delay
- Transaction Network Round Trip Time
- Transaction Network Volume
- Transaction Web Errors
- User Logon Counts
- User Logon Details
- User Logon Details for a User Group
- User Summary for a User Group

- Visited Sites
- XenApp Summary
- XenApp System Performance Archive
- XenApp User Summary

The following reports display data for XenApp 5.0 or XenApp 5.0 Feature Pack 2, and XenApp 6.0, but not for Presentation Server 4.5:

- Application Response Failures
- Application Response Time
- Application Response Time for a Test
- HDX MediaStream I/O
- HDX Plug-n-PLay I/O
- Session Duration
- Session Duration for a User Group
- XenApp Server Utilization

Agent Data Collection

The following table shows which types of data are collected by an agent in Advanced Mode, listed by XenApp version:

Data Type	CPS 4.5	XenApp 5.0 or XenApp 5.0 Feature Pack 2	XenApp 6.0
Application Errors	X	X	X
Application Not Responding	X	X	X
Session Performance	X	X	X
System Performance	X	X	X
Custom Performance Monitoring	X	X	X
Device Asset Changes	X	X	X
Disk Usage	X	X	X
Light Trace Events	X	X	X
Network Performance	X	X	X
Network Transactions	X	X	X
Process Crashes/Snapshots	X	X	X

Data Collection by Presentation Server or XenApp Server Version

Process Performance	X	X	X
Process Usage	X	X	X
Remote Agent Access	X	X	X
System Performance	X	X	X
EUEM Data	X	X	X
ICA Channel Performance	X	X	X
IMA Service State	X	X	X
Print Services *	X	X	X
Active Application Monitoring		X	X

* Due to high performance costs, printer tracking is disabled by default when you install the agent. This means that ICA Printer I/O report will not contain printer name or printer driver information. To enable printer tracking, set the following registry setting to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\System  
Monitoring\Agent\Ctrx\4.00\DisablePrinterTracking
```

Once printer tracking is enabled, this setting will be preserved during upgrades of the EdgeSight for XenApp agent.

Integrating EdgeSight Alerts with Microsoft System Center Operations Manager

You can deploy and configure software to forward EdgeSight alerts to Microsoft® System Center Operations Manager 2007 (SCOM) and to monitor the health of EdgeSight Servers. The required software includes the Citrix EdgeSight Management Pack and EdgeSight Server 5.2 or later. Currently, only alerts generated by EdgeSight for XenApp agents can be forwarded.

About the Citrix EdgeSight Management Pack

The Citrix EdgeSight Management Pack, along with the EdgeSight alert actions feature, facilitates alert forwarding from an EdgeSight Server to SCOM. The Management Pack also includes monitors, rules, views, and tasks for monitoring the health of Citrix EdgeSight Servers.

When you import the EdgeSight Management Pack, it discovers all EdgeSight Servers and implements rules that receive and display the alerts forwarded by the EdgeSight Server.

EdgeSight Management Pack includes the following features:

- Collects and displays alerts forwarded by EdgeSight Server
- Monitors the health of the Citrix RSSH Admin and Citrix RSSH Application Manager services
- Remotely restarts the Citrix RSSH Admin and Citrix RSSH Application Manager services if they are stopped
- Collects EdgeSight errors written to the Application Event Log on the EdgeSight Server
- Provides multiple methods to launch the EdgeSight Server Console from within the Operations Manager console

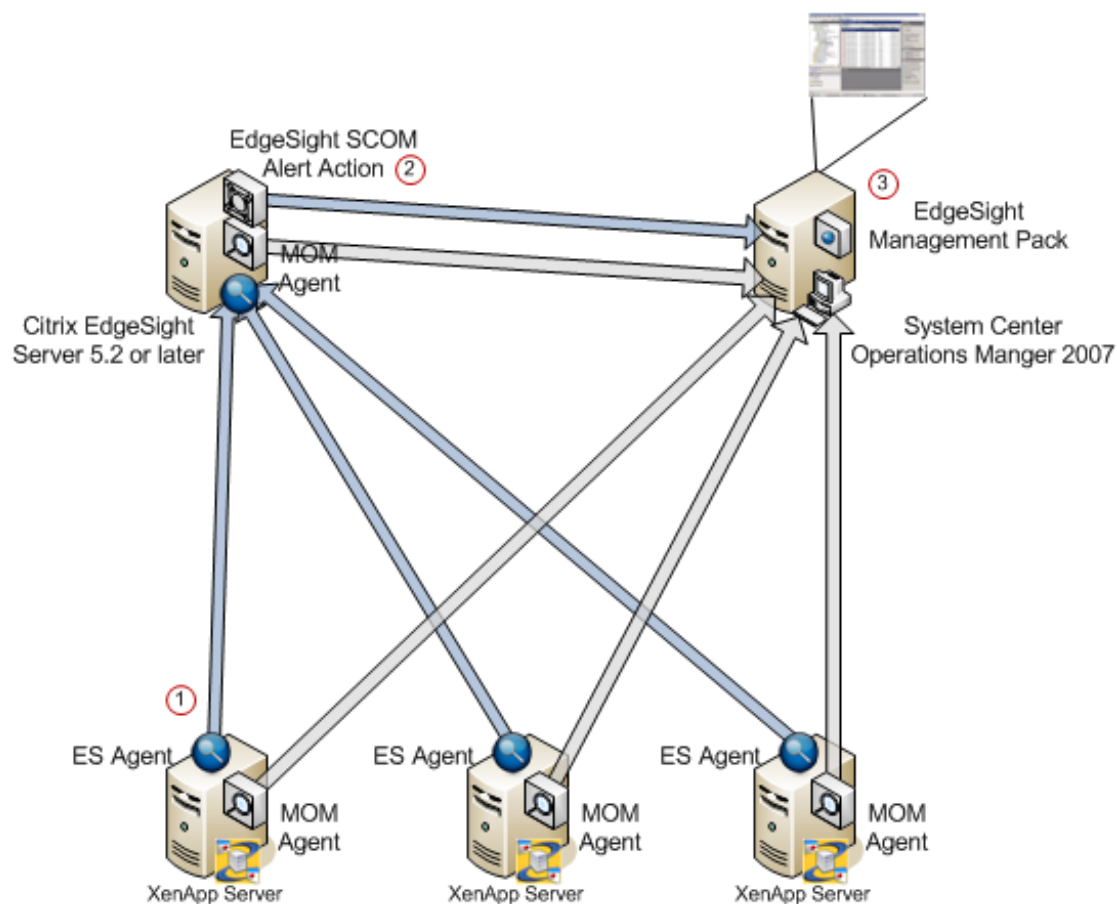
About the Forward to Microsoft System Center Operations Manager Alert Action

The EdgeSight alert actions feature is used to forward EdgeSight Alerts to the Operations Manager Root Management Server. The Forward to Microsoft System Center Operations Manager alert action allows you to specify an alert name, a root management server, and a set of credentials for authentication to that server.

Deployment Diagram

The following diagram illustrates communications between Citrix EdgeSight Server and SCOM. The EdgeSight Management Pack workflow is as follows:

1. The EdgeSight agent running on a XenApp server detects an error condition and sends an alert to the EdgeSight Server
2. An alert action on the EdgeSight Server forwards the alert to SCOM
3. The EdgeSight Management Pack, within SCOM, receives the EdgeSight alert and displays it in the Operations Manager Console; aggregating EdgeSight alerts with SCOM alerts into one logical view



System Requirements for EdgeSight Alert Integration with System Center Operations Manager

Citrix EdgeSight alert integration with System Center Operations Manager requires the Citrix EdgeSight MP file that you import into Operations Manager from the Operations Console.

Operations Manager 2007 Server

To use the Management Pack, you must be running Operations Manager 2007. The Operations Manager 2007 minimum hardware and software requirements can be found here: <http://www.microsoft.com/systemcenter/operationsmanager/en/us/system-requirements.aspx>.

You must import the Citrix XenApp Management Pack v5.0 into Operations Manager prior to importing the EdgeSight Management Pack. The XenApp Management Pack is available on the XenApp Server Enterprise and Platinum Edition DVD or by download at www.citrix.com.

It is important to import the XenApp Management Pack files into Operations Manager in the following order:

1. Citrix.Library.mp
2. Citrix.PresentationServer.mp

The Citrix.LicenseServer.mp is also part of the XenApp Management Pack, but is not required by the EdgeSight Management Pack.

Note: Be sure to configure a Citrix Administrator Account “Run As Profile” with the Citrix administrator credentials after your import Citrix.PresentationServer.mp. Failure to complete this step can prevent Citrix servers from appearing in the Citrix Managed Servers group. See the *Management Pack for Operations Manager 2007 Administrator's Guide*, for XenApp 5.0 for Windows Server 2008 at <http://support.citrix.com/article/CTX116421> for detailed instructions.

XenApp 5 and Presentation Server 4.x Servers

You must install the Operations Manager Agent and the Citrix EdgeSight for XenApp Agent on all XenApp and / or Presentation Servers as described in *How to Deploy the Operations Manager 2007 Agent Using the Agent Setup Wizard* (<http://technet.microsoft.com/en-us/library/bb309515.aspx>).

Ensure the Citrix servers are properly discovered and monitored in both EdgeSight and Operations Manager.

EdgeSight Server

You must install the Operations Manager Agent on the EdgeSight Server to allow Operations Manager to discover and monitor the server, as well as receive alerts from the EdgeSight

Server. Installation procedures are provided in as described in *How to Deploy the Operations Manager 2007 Agent Using the Agent Setup Wizard* (<http://technet.microsoft.com/en-us/library/bb309515.aspx>).

You must also install the Operations Manager Console which includes libraries required for EdgeSight Server to communicate with the Operations Manager Root Management Server, as described in *How to Deploy an Operations Manager 2007 Operations Console Using the Setup Wizard* (<http://technet.microsoft.com/en-us/library/bb381292.aspx>).

Prerequisites Review

Note: These prerequisites are listed in the order in which they must be imported or installed.

Operations Manager 2007 Server

- Import Citrix.Library.mp
- Import Citrix.PresentationServer.mp

XenApp Servers

- Install EdgeSight Agent
- Install Operations Manager Agent

EdgeSight Server

- Install Operations Manager Agent
- Install Operations Manager Console or Operations Manager Authoring Console

Installing and Configuring Components

To integrate EdgeSight software with the System Center Operations Manager, you must complete the following tasks:

- Import the EdgeSight Management Pack
- Configure an alert action to forward alerts to SCOM
- Assign the alert action to an alert rule

Importing the EdgeSight Management Pack

1. Open the EdgeSight media, click on **Browse CD**, and go to `\installers\Management_Packs`.
2. Locate the file named `Citrix.EdgeSight.mp` and copy it to the default Management Pack folder (`%ProgramFiles%\System Center Management Packs\`) on any machine running the Operations Manager Console.
3. Log on to the Operations Manager server and open the Operations Console.
4. Select **Administration** in the view pane Select Management Packs from the Administration View.
5. Select **Import Management Pack(s)** from the Actions menu.
6. Browse to the `Citrix.EdgeSight.mp` Management Pack file and click **Open** to view the Import Management Packs dialog box.
7. Click **Import**.
8. After the Management Pack is successfully installed, Operations Manager automatically deploys it to all the managed computers in your management group. Please allow time for this process to complete.

Configuring the Alert Action

To configure Citrix EdgeSight Server to forward alerts to SCOM:

1. Launch the EdgeSight Server Console.
2. Click the **Configure** tab.
3. Under Company Configuration select **Alerts > Actions**.
4. Click the **New Alert Action** button.

5. Select the **Forward to Microsoft System Center Operations Manager** option and then click the **Next** button to start the Alert Actions Creation Wizard
6. If you want to use an existing configuration (root management server name and credentials), select one from the drop-down menu. Otherwise, proceed to the next step.
7. Enter the name or IP address of the Root Management Server for System Center Operations Manager. A fully qualified domain name (FQDN) is only required in those cases where it is needed to establish a connection between the EdgeSight Server and the Root Management Server.
8. Enter the credentials to be used when authenticating to the server.
9. Click the **Next** button once the Alert Action properties are set.
10. Review the Alert Action and then click **Finish** to save.

Once the alert action is created you must assign it to an alert rule.

Assigning the Alert Action to an Alert Rule

1. Click the **Configure** tab.
2. Under **Alerts > Rules.**, click on the edit icon of an existing alert rule to launch the Alert Rules Wizard.
3. Select **Change Alert Rule to Alert Action Mappings** and click the **Next** button.
4. On the Assign Alert Rule to a Department screen, select **All** or a specific department you want to assign this rule to, and click the **Next** button.
5. On the Assign Action to Alert Rule screen, pick **Select the Alert Actions** radio button, check the alert action you created in the previous section, and click the **Finish** button

Uninstalling the EdgeSight Management Pack

You can uninstall the Management Pack using the Operations Manager Console. Uninstalling the Management Pack removes all the references to it from the Operations Manager database, including the monitoring objects provided by the Management Pack along with any dynamically discovered event, performance, or alert data. For information about uninstalling management packs, see your Operations Manager documentation.

Using the Management Pack

This topic introduces you to the Citrix EdgeSight views, rules, monitors, and tasks that are included in the Management Pack. It explains how to configure the Management Pack for your site. The topics include:

- Citrix Managed Objects
- Citrix Views
- Starting the Citrix EdgeSight Management Console

About Citrix Managed Objects

The Citrix family of Management Packs monitors and reports on a number of Citrix-specific objects.

Object	Description
Citrix Deployment	Represents a discovered Citrix deployment that can consist of multiple farms, zones, and EdgeSight Servers
Citrix Managed Server	Represents a XenApp or Presentation Server monitored by Operations Manager. A managed server must be a server that is running a version of Presentation Server listed in “Citrix XenApp Server Managed Computers” (next) with an appropriate license. The server must also be running the Presentation Server Provider.
Citrix Unsupported Server	Represents a server not monitored by Operations Manager. An unsupported server is not running a version of Presentation Server listed in “Citrix XenApp Server Managed Computers” (next).
Citrix Unlicensed Server	Represents a server not monitored by Operations Manager. The server is running the Presentation Server Provider, but is unlicensed or missing a valid license. Note that Operations Manager checks the licenses on these servers hourly.
Citrix EdgeSight Server	Represents an EdgeSight Server monitor by Operations Manager. The server must be running EdgeSight for XenApp 5.0 or later with an appropriate license.
Citrix Server Application	An abstract class that represents a server running any Citrix server product. The Citrix Server Application class is the target for alerts forwarded by EdgeSight.

Citrix XenApp Server Managed Computers

In the Management Pack, a Citrix XenApp Server (displayed as Citrix Presentation Server) managed computer is a server that is running one of the following releases of Presentation Server with an appropriate license:

- Citrix Presentation Server 4.0, Enterprise Edition
- Citrix Presentation Server 4.5, Enterprise or Platinum Edition
- Citrix XenApp Server 5.0, Enterprise or Platinum Edition

Servers running earlier versions of Presentation Server are considered unsupported computers, while servers that are not appropriately licensed are considered unlicensed computers. These computers are not monitored by the Management Pack, and will not appear in the deployment topology diagram.

Note: After licenses are allocated, computers running Presentation Server might not be recognized as managed until the next time Attribute Discovery runs. By default, this happens every 60 minutes.

About Citrix Views

The EdgeSight Management Pack inherits from, and integrates with, Citrix views available in the Citrix XenApp Management Pack. These views allow you to monitor events raised by both Operations Manager and EdgeSight for servers and server farms running Citrix XenApp and Presentation Server.

The Citrix EdgeSight Management Pack extends the Citrix Active Alerts view, All Citrix Events view, Citrix Deployment State view, and the Citrix Presentation Server Topology Diagram view. It also adds the Citrix EdgeSight folder which contains the Citrix EdgeSight Alerts view, the Citrix EdgeSight Console View, and the Citrix EdgeSight State view. The Citrix Performance view and Citrix Licensing view are not affected by the EdgeSight Management Pack.

Alert and Event Views

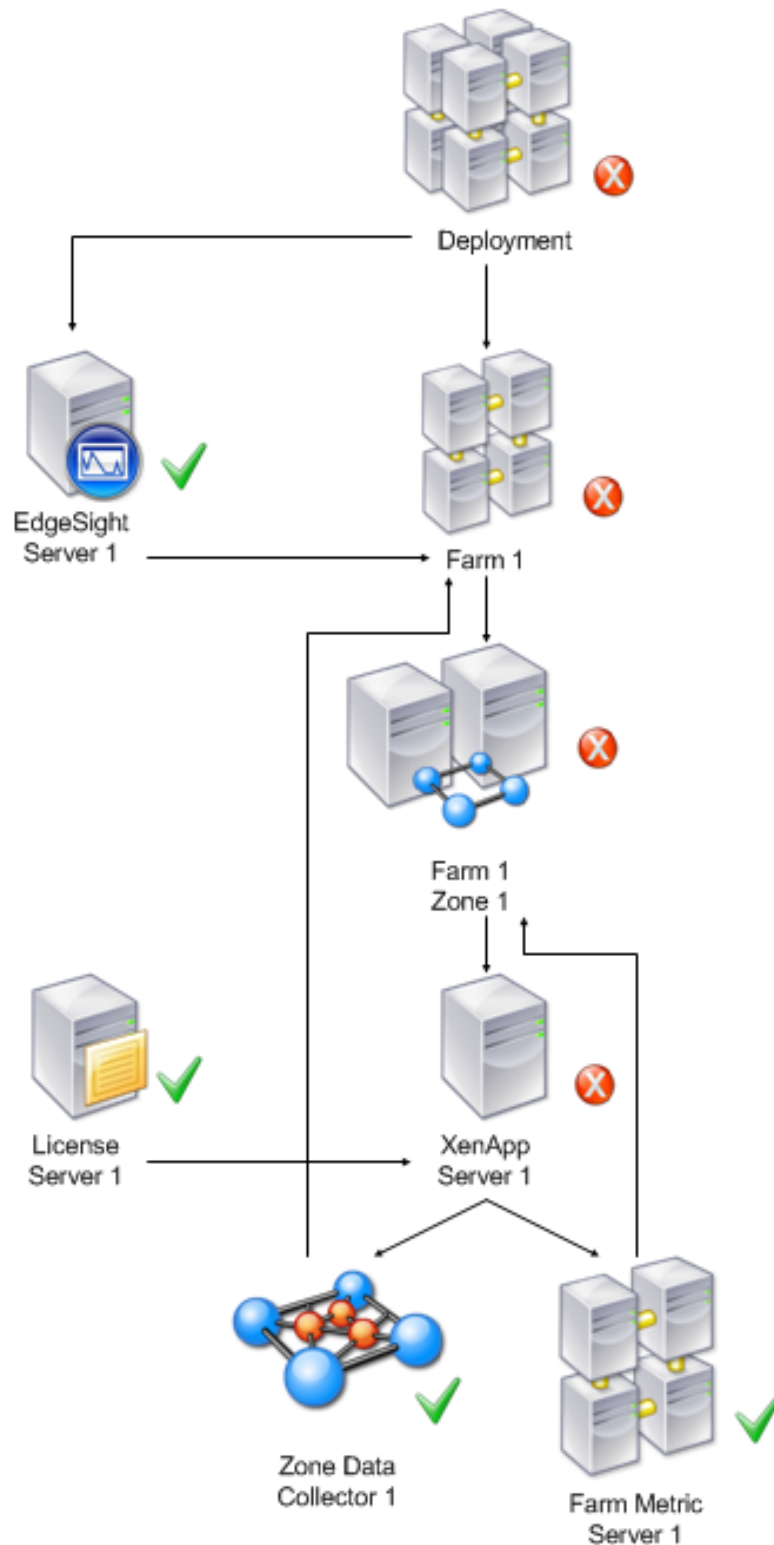
Alert and event views provide system administrators with real-time event and alert information. Alert views group alerts by severity, and event views sort events chronologically for ease of reference.

Alerts and events generated by the XenApp Management Pack rules and monitors and alerts forwarded by the EdgeSight Server are collected and displayed in these views. There are three Citrix alert and event views.

View	Description
All Citrix Events	Displays all the events raised by Citrix Presentation Server components and all events inserted by the EdgeSight alert actions on managed servers.
Active Alerts from Citrix Servers	Displays all unresolved alerts raised against managed servers by all management packs (not only the XenApp Management Pack).
Active Citrix Alerts	Displays all unresolved alerts raised by the XenApp Management Pack and by the EdgeSight Management Pack.

Citrix Server Topology Diagram View

The Citrix Server topology diagram view provides a hierarchical representation of a Citrix deployment, displaying farms, zones, license servers, XenApp Servers, and EdgeSight Servers and their relationships.



The topology view provides the following information:

- The name of the farm, zone, or server and the discovered properties of each object. The discovered properties of the EdgeSight Server object are:
 - EdgeSight Version Number
 - SQL Server Name
 - Database Name
 - Database Version
 - IP Address
 - EdgeSight admin console URL
 - Web Port
 - Last Update
- The current alert state, propagated up the tree so that state changes are visible even when the view is collapsed.

Citrix EdgeSight Folder

The EdgeSight Management Pack creates a new Citrix EdgeSight folder under the Citrix Presentation Server root folder. The Citrix EdgeSight folder contains an alert view, console view, and state view that contain information specific to the EdgeSight Server.

View	Description
Citrix EdgeSight Alerts	Displays all alerts raised by the alert action feature running on the EdgeSight Server.
Citrix EdgeSight Servers	Displays all the discovered Citrix EdgeSight Servers and their current health state.

Citrix EdgeSight Server Health Roll-up

Monitors represent the health state of a managed computer by evaluating rules against pre-defined criteria. The health state can be set to one of three conditions: Success, Warning, and Critical.

The EdgeSight Management Pack contains two Windows service monitors; one for the Citrix RSSH Admin Service and one for the Citrix RSSH Application Manager Service.

Monitor	Description
Citrix RSSH Aggregate	Health Roll-up Policy that displays the worst health state of the two RSSH Service monitors.

Citrix RSSH Admin Service	Monitors the state of the Citrix RSSH Admin Service. The health state is set to Critical when this service is stopped and Healthy when the service is running. The Monitor also includes a recovery task that will remotely restart the service and reset the monitor state when after recovery finishes.
Citrix RSSH Application Manager Service	Monitors the state of the Citrix RSSH Application Manager Service. The health state is set to Critical when this service is stopped and Healthy when the service is running. The Monitor also includes a recovery task that will remotely restart the service and reset the monitor state when after recovery finishes.

Starting the Citrix EdgeSight Console

To aid troubleshooting alerts forwarded to Operations Manager by EdgeSight Server, the EdgeSight Management Pack provides multiple ways to launch the EdgeSight Management Console from the Operations Manager console.

To start the EdgeSight Console:

1. Log on to the Operations Manager Console.
2. Navigate to the Monitoring View.
3. Perform one of the following:
 - In the Citrix Presentation Server Topology Diagram view, select an EdgeSight server icon, in the Detail View click on the EdgeSight Console URL property value or in the Actions pane, select **Start EdgeSight Management Console**.
 - In the Citrix EdgeSight Servers view, select an EdgeSight server, in the Detail View click on the EdgeSight Console URL property value or in the Actions pane, select **Start EdgeSight Management Console**.

Security Considerations

This topic provides information about Operations Manager actions accounts and using low-privilege accounts with the Citrix EdgeSight Management Pack and the SCOM alert action.

EdgeSight Management Pack

The EdgeSight Management Pack uses the default agent action account that is created when Operations Manager is first installed to perform discovery and run rules, tasks, and monitors. By default, Operations Manager assigns the Local System account as the agent action account. When running as Local System, the agent action account has all the privileges necessary to perform discovery and run rules, tasks, and monitors.

Low-Privilege Environments

You can use a low-privilege account for the agent action account; however the service recovery tasks require elevated rights. The low-privilege account must meet the following requirements:

- Member of the local users group
- Granted Log On Locally rights

With the low-privilege action account the following features are supported:

- EdgeSight Server Discovery
- EdgeSight RSSH service monitoring
- Launch the EdgeSight Console

With the low-privilege action account the following features are not supported:

- Recovery task to restart the Citrix RSSH Admin Service
- Recovery task to restart the Citrix RSSH Application Manager Service

EdgeSight Alert Action

The Alert Action includes credentials used for authentication. This account must be a member of the Operations Manager Administrators role to access the SDK Service. This account must also be a member of the administrator's Local Group on the EdgeSight Server so that the alert action can spawn a local process. The low-privilege section describes the minimum permissions required by this account.

Low-privilege Environments

The minimum privileges required by the SCOM administrator account are:

- Domain: Member of the Domain Users Global Group
- Operations Manager: Member of the Operations Manager Administrators role
- EdgeSight for XenApp 5.0: Member of the Administrator Local Group on the EdgeSight Server

Troubleshooting EdgeSight

Troubleshooting License Server Monitoring

By setting the Polling Errors option to **Send Email** on the License Servers page (**Configure > License Monitor Configuration > License Server**), you can ensure that email is sent to the EdgeSight Administrator if license server polling fails. The administrator has several options for gathering more information:

- Examine license server-related messages
- Examine the log file for the core_lsm_license_poller server script

In addition, license servers with polling errors are indicated by specific error or warning icons in the License Usage Summary and License Usage Trending reports available on the **Track Usage** tab. For more information on these reports, see the “License Usage Summary” and “License Usage Trending” topics in online help.

License Server Monitoring Messages

You can display license server monitoring messages on the Messages page (**Server Status > Messages**). To isolate the messages, sort the messages by source and locate those with a source of License Server Monitor. Most of the messages relating to license server monitoring are information and reflect actions taken on the EdgeSight Server, such as adding or deleting a license server configuration. These information messages include:

- New License Server Added
- License Server Deleted
- License Server was disabled
- License Server was re-enabled
- New Product Feature Code found on license server

The Polling Failed error message indicates that an attempt to poll a license server has failed, most likely due to the inability of the license server poller to connect to the license server. (In most cases, an error code of -96 is displayed.) The failure to connect could be due to the license server being down or a network problem.

License Server Poller Log File

You can display the license server poller log file on the Server Script Host page (**Server Status > Server Script Host**). Locate the core_lsm_license_poller script, right-click the menu button, and select **View Log**.

A normal polling sequence with no errors is similar to the following:

```
1/20/2010 8:12:36 PM: LicenseServerMonitor: OnTimer: begin
1/20/2010 8:12:36 PM: LicenseServerMonitor: PollLicenseServers: begin
1/20/2010 8:15:49 PM: LicenseServerMonitor: PollLicenseServers method invoked *****
1/20/2010 8:15:49 PM: LicenseServerMonitor: Begin polling Server LICSERVER01.mycompany.net on port 2700
1/20/2010 8:15:49 PM: LicenseServerMonitor: Total Polling Time: 0:0.93
1/20/2010 8:15:49 PM: LicenseServerMonitor: Polling Successful. Total Licenses Retrieved: 21
1/20/2010 8:15:49 PM: LicenseServerMonitor: Begin polling Server LICSERVER02.mycompany.net on port 2700
1/20/2010 8:15:49 PM: LicenseServerMonitor: Total Polling Time: 0:51.750
1/20/2010 8:15:49 PM: LicenseServerMonitor: Polling Successful. Total Licenses Retrieved: 300
1/20/2010 8:15:49 PM: LicenseServerMonitor: PollLicenseServers method completed. *****
```

An error in polling is logged as follows:

```
1/20/2010 9:26:31 PM: LicenseServerMonitor: Begin polling Server LICSERVER01.mycompany.net on port 2700
1/20/2010 9:26:31 PM: LicenseServerMonitor: Total Polling Time: 0:10.0
1/20/2010 9:09:18 PM: LicenseServerMonitor: Polling Failed. Error code: -96
1/20/2010 9:09:18 PM: LicenseServerMonitor: Error Message: 1/20/2010 9:07:06 PM: The License Server Monitor
cannot retrieve any license utilization data for server "LICSERVER01.mycompany.net", port 27000.
Contact your Citrix License Server Administrator.
```

Forward the log to your Citrix License Server Administrator for further investigation.

Troubleshooting Using Agent Log Files

There are several log files located on devices running the agent which can be used to help diagnose issues of agent to server communication. Note that for agents running on virtual desktops, the log files are copied to an agent data file share specified during agent installation.

- The system and application event logs (found in the event viewer)
- The main EdgeSight log file. The default location is:

```
%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\SYS_EVENT_TXT.txt
for Microsoft Vista and Windows 2008 systems
```

```
%ALLUSERSPROFILE%\Application Data\Citrix\System
Monitoring\Data\SYS_EVENT_TXT.txt for all other systems
```

- Individual worker log files. (See “Monitoring Workers” in [Configuring, Scheduling, and Running Workers](#) for more information on worker log files.) The default location is:

```
%ALLUSERSPROFILE%\Citrix\System Monitoring\Data\EdgeSight\log for
Microsoft Vista and Windows 2008 systems
```

```
%ALLUSERSPROFILE%\Application Data\Citrix\System
Monitoring\Data\EdgeSight\log for all other systems
```

If you detect a problem that you cannot solve and need to contact Technical Support, please have the agent and server software version numbers at hand. To verify product

version information:

- Agent: Open the SYS_EVENT_TXT file. When the agent starts up, it inserts a line similar to the following:

----- Starting Agent on machinename version 5.0.74.0 -----

- Server: Open the EdgeSight console and navigate to **Server Status > About**. The correct version is listed next to Reflectent.EdgeSight.Loader.dll.

EdgeSight for Load Testing 3.8

EdgeSight for Load Testing is an automated load and performance testing solution for Citrix XenApp and XenDesktop environments.

In This Section

Under this node, you will find the following resources for EdgeSight for Load Testing:

About this release	Known issues in this release
System requirements	System requirements for this release
Install	Installation procedures
Administer	How to use EdgeSight for Load Testing

EdgeSight for Load Testing 3.8

EdgeSight for Load Testing is an automated load and performance testing solution for Citrix XenApp and XenDesktop environments.

In This Section

Under this node, you will find the following resources for EdgeSight for Load Testing:

About this release	Known issues in this release
System requirements	System requirements for this release
Install	Installation procedures
Administer	How to use EdgeSight for Load Testing

About EdgeSight for Load Testing 3.8

About this Readme Version: 1.3

For the latest critical updates for Citrix products, see <http://support.citrix.com>.

Getting Support

Citrix provides technical support primarily through Citrix Solutions Advisors. Contact your supplier for first-line support or use Citrix Online Technical Support to find the nearest Citrix Solutions Advisor.

Citrix offers online technical support services on the [Citrix Support Web site](#). The Support page includes links to downloads, the Citrix Knowledge Center, Citrix Consulting Services, and other useful support pages.

EdgeSight for Load Testing 3.8 Service Pack 1

This release provides a number of security enhancements to the product. (For more information on these changes, see <http://support.citrix.com/article/CTX129699>.) No new end user features have been added for this release and no changes are required to tests or scripts. When upgrading from EdgeSight for Load Testing 3.8, keep in mind the following:

- The user will be prompted to reset the security password during installation. This occurs when installing the Controller, the Launcher, or both components.
- Both the Controller and Launcher components must be upgraded. If an old Controller is used with a new Launcher, the following error message is displayed in the Controller: One or more Launchers have reported an error and have exited. If a new Controller is used with an old Launcher, no error message is passed to the Controller. However, the error is logged in the trace/lbservice.txt file located on the machine running the Launcher. For example: ControllerConnection. ControllerListen. Unrecognized message from Controller.

When establishing connections using ICA files, it is recommended that the ICA files be on the systems where the Launcher is running rather than on a remote file share.

Known Issues in EdgeSight for Load Testing 3.8

- Some synchronization point instructions require a preceding idle time instruction. Synchronization Point instructions with a type of "Changed" must be preceded by a Synchronization Point instruction with a type of "Exists." The first Synchronization Point instruction ("Exists") requires a preceding Idle Time instruction in order for the synchronization points to function properly. For example, a properly formed script would have the following instruction sequence:

Idle Time

Sync Point (Type "Exists")

Idle Time

Sync Point (Type "Changed")

Workaround: Edit the script to add an Idle Time instruction before all Synchronization Point instructions with a type of "Exists" which precede a Synchronization Point instruction with a type of "Changed." To check the Synchronization Point type, click on the instruction in the Test Tree and examine the Type as shown in the main window.

- Synchronization point timeouts may occur in older tests. Tests created with versions of EdgeSight for Load Testing prior to version 3.8 might experience synchronization point timeouts when a type of Match or Search is used.

Workaround: If bitmap Match or Search sync points time out, you may need to re-record the test to correctly capture the client screen color depth.

- Password Reset Tool Requires Administrator Privileges. The password reset tool must be run with unrestricted administrator privileges. If the user does not have administrative privileges, the password cannot be reset.
- Replaying Tests with An Evaluation License Requires Administrator Privileges. The Controller must be run with unrestricted administrative privileges to replay tests when using an evaluation license. If the user does not have administrative privileges, an insufficient privileges error is displayed.
- Edited Tests Overwrite Original Tests When Replayed. Currently, if there are changes to a test, the original test is overwritten with the revised test when the test is replayed. (Saving the test on replay allows the creation of temporary copies which can help recover the test in case of a crash.) If you want to preserve the original test, save the original test with another name before replay.
- Temporary ICA File Can Omit Entries. When using an ICA file for a connection, a wfcrun32 error can occur stating that the application cannot be launched. This is due to missing entries in the temporary ICA file.

Workaround: Add the following entries to the ICA file:

- [WFClient]

 HttpBrowserAddress= *servername:port*
-

[publishedAppName]

Address= publishedAppName

- **Launcher Log Access.** In order to access the logs created by the Launcher, a user must have access to the installation user's Documents folder.
- **Non-ASCII Window Title Display Issues.** Non-ASCII window title strings may not display correctly when recording using XenApp 5.0 and Citrix Online Plug-in 11.0. If you wish to use this configuration, please update to Online Plug-in 11.1 or higher.
- **Windows Authentication Security IIS Role Required by EdgeSight Web Interface Support.** The Windows Authentication Security IIS role is required for the EdgeSight Web Interface Support components. Because the installer does not currently verify the presence of the role, you should check the target machine to ensure that the role is present.
- **Web Interface Upgrade Can Result in EdgeSight for Load Testing Not Working.** If the Web Interface component is upgraded on a XenApp server or Presentation Server, this can interfere with normal EdgeSight for Load Testing operation.

Workaround: After the Web Interface component is upgraded on a XenApp server or Presentation Server, reinstall the associated EdgeSight for Load Testing instance.

- **Long Running Tests with Short Connections Times Can Consume Large Amounts of Memory.** For some long running tests with very short connection times and for tests that consistently fail to connect, the systems that Launchers are running on may consume large amounts of memory. In these cases, the amount of memory available on the Launcher should be monitored throughout the test.
- **The Online Plug-in 11 can Cause TUser Window Freeze.** In some cases on Windows 2008 systems using the Online Plug-in 11 , a high rate of new connections can cause TUser windows to freeze during the connection phase, displaying a white screen. These frozen windows will block a test from ending gracefully. To close these unresponsive windows, simply close the Launcher on the faulty machine. To work around this problem, increase the throttling values in the Test Configuration Properties, slow the rate of increase within the load, or distribute the load across a greater number of launcher machines.

System Requirements for EdgeSight for Loading Testing 3.8

The requirements for systems running the EdgeSight for Load Testing Controller and Launcher are listed in the following table.

Controller and Launcher Requirements	
OS	<p>Controller</p> <p>Microsoft Windows Vista, Microsoft Windows XP, Microsoft Windows 7, Microsoft Windows Server 2003, Microsoft Windows Server 2008, and Microsoft Windows Server 2008 R2 (32-bit and 64-bit systems on all operating systems)</p> <p>Launcher</p> <p>Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows Server 2003 (32-bit systems only), Microsoft Windows Server 2008, and Microsoft Windows Server 2008 R2 (32-bit and 64-bit systems on all operating systems except as noted)</p> <p>Citrix License Server for Windows 4.5 or higher</p> <p>ICA Client Version 10 or higher for load testing XenApp systems</p> <p>ICA Client Version 12.1 or higher for load testing XenDesktop 5 systems</p> <p>Target systems include Citrix Presentation Server 4.0 or higher, Citrix XenApp 5.0 or 6.0, and Citrix XenDesktop 5.0</p> <p>Microsoft Excel (for displaying Log files)</p> <p>.NET Framework 3.5 or later is required for all Launchers and Controllers that will be establishing connections using the Web Interface.</p> <p>Visual J# Version 2.0 (if using XML Interface Connector)</p>
CPU	2 gigahertz (GHz) or faster CPU

Memory	1 gigabyte (GB) of RAM
Disk	1 gigabyte (GB) of free space

Important: When running the Controller on a Windows Server 2003 64-bit system and logging in via RDP, you must run RDP and log in to session 0 in order for the Controller to be detected and for the recording window to be visible. Refer to your platform documentation for the specific command line required to log in to session 0.

Requirements for EdgeSight Web Interface Support

The EdgeSight Web Interface Support software is designed to be deployed on machines running Web Interface 4.5 or higher up to Web Interface 5.4. The target machine must meet the requirements listed in the Web Interface product documentation. In addition, the Windows Authentication Security IIS role is required.

Requirements for Citrix License Server for Windows

EdgeSight for Load Testing requires Citrix License Server for Windows 4.5 or higher. If the license server is not installed and running, [license information](#) cannot be obtained and Citrix EdgeSight for Load Testing is not allowed to start Launchers. You will receive instructions by email for downloading EdgeSight license keys. If you are unfamiliar with the Citrix License Server, you should start by reading [Licensing Your Product](#).

When installing the license server, accept the defaults provided by the MSI file for the destination folder and the license file location. When selecting features, you can choose whether to select the License Management Console; this feature is not required, but may be useful in managing your licenses.

Obtaining the MSI Files

Citrix EdgeSight software is distributed both electronically and on media, depending on the specific product purchased. Consult with your sales representative for more information.

Installation Overview

Citrix EdgeSight for Load Testing software is installed using the following Windows Installer (MSI) files:

- EdgeSight for Load Testing.msi
- ESLT WI Support.msi

Note: Do not modify the base MSI file. Modifying the base MSI file can interfere with support efforts in case of installation issues.

The EdgeSight for Load Testing MSI file installs the following components of the EdgeSight for Load Testing software:

- EdgeSight for Load Testing Controller—Used to record and create virtual user scripts and define tests. When the test is ready for playback, the Controller instructs the Launchers to run the test with a certain number of virtual users for a certain period of time. The default installation location for the Controller is %ProgramFiles%\Citrix\Citrix EdgeSight for Load Testing.
- EdgeSight for Load Testing Launcher—Receives the commands from the Controller and generates virtual user ICA sessions on the target systems. The number of Launchers required will vary based on the target virtual user load. Launchers report session information back to the Controller for runtime and post run-time analysis. The Launcher is installed as a service (Citrix EdgeSight Launcher Service). The default installation location for the Launcher is %ProgramFiles%\Citrix\Citrix EdgeSight Simulation.
- XML Interface Connector—Allows users to connect to applications made available through the XML Service. The default installation location for the connector is %ProgramFiles%\Citrix\Citrix EdgeSight Xen Connector. This feature requires the Visual J# Version 2.0 Redistributable Package available from Microsoft at <http://msdn2.microsoft.com/en-us/vjsharp/default.aspx>.

Launchers are installed on clients of the servers that will be under test. They can be installed on systems with the Controller and as stand-alone Launchers.

The EdgeSight Web Interface Support MSI file installs the following components on top of the Web Interface (WI) deployment, facilitating access to the WI published resources:

- Application Page—An application-specific page (for example, Citrix/AccessPlatform/site/eswi.aspx) is installed on the Web Interface Server of the system you are load testing. You must correctly identify the location of the Application Page when configuring the Web interface.
- EdgeSightWISecurity group—Created on the target system to control access to the EdgeSight Web Interface page. All users who will be logging on to the Controller or Launcher computers should be added to this group.

If you do not want to add the Controller and Launcher login user accounts as members of the EdgeSightWISecurity group, you can alternatively use the Web Interface Access

Credentials dialog to specify a set of credentials to be used in accessing the Application Page. When running a test, the ICA file is retrieved from the Web Interface using the user account under which the Launcher is running (if Web Interface access Credentials are not specified), or the specified Web Interface access credentials. When you browse the Web Interface from the Controller, the same access scheme applies. See “Web Interface Application Browser” in the Controller online help for more information on setting these credentials.

- **Web Interface Connector**—Allows EdgeSight for Load Testing users to connect to applications made available through the Citrix Web Interface. The default installation location for the connector is %ProgramFiles%\Citrix\Citrix ESLT Web Interface XML Service Connector.

Citrix EdgeSight for Load Testing Licensing

When a test is replayed, the EdgeSight for Load Testing software checks for the presence of a XenApp or XenDesktop Platinum or Enterprise license on the specified licensing server. If a valid license is detected, you can run as many users as required.

If you do not have a XenApp or XenDesktop Platinum or Enterprise license on the specified licensing server, but have CCU licenses, the number of users you can test with is limited by the amount for which you are licensed. If no licenses of any kind are detected, the software displays the message "Could not find a valid license on the designated license server" and offers to run in 15 user evaluation mode.

Citrix EdgeSight for Load Testing licensing is provided by the Citrix License Server for Windows. See [Citrix License Server for Windows Requirements](#) for information on obtaining the license server documentation.

If you are using CCU licenses, once you download license files (CES_*.lic), manually place them in the MyFiles folder of the license server directory, for example: %ProgramFiles%\Citrix\Licensing\MyFiles. These files will need to be in place prior to running load tests.

To Install the EdgeSight for Load Testing Components

You can install this release of EdgeSight for Load Testing as a direct upgrade from Version 3.0 or higher, or as a clean installation by first removing the older version. A clean installation creates the Alarms, Debug, ICA Files, Logs, Reports, Tests, and Tmp folders in My Documents\Citrix EdgeSight for Load Testing. An update maintains the folders in the original folders, %ProgramFiles%\Citrix\Citrix EdgeSight for Load Testing\.

Note: Before performing an upgrade, back up all scripts.

The EdgeSight for Load Testing software supports installation from media or by directly invoking the MSI user interface. Use the following steps to install the EdgeSight for Load Testing software:

1. If you are installing from media, insert the media. Click on **EdgeSight for Load Testing Installation**. If you are installing directly from the MSI file, double click the EdgeSight for Load Testing MSI file to start the setup wizard. The Welcome screen is displayed.
2. Click **Next** to continue. The End-User License Agreement screen is displayed.
3. After reading the license, select **I accept** and click **Next**. The Choose Setup Type screen is displayed.
4. Select the type of installation you want to perform and click **Next**.
 - a. **Typical** - Install the Controller and Launcher.
 - b. **Custom** - Select the components you want to install from Controller, Launcher, and Web Interface XML Service Connector. The Web Interface XML Service Connector is installed on the same machine as the Controller and Launcher and allows users to connect to applications made available through the XML Service. This feature requires the Visual J# Version 2.0 Redistributable Package available Chapter 2 Installing EdgeSight for Load Testing 11 from [Microsoft website](#).
 - c. **Complete** - Install the Controller, Launcher, and Web Interface XML Service Connector.
5. Click **Install** to install the software. The Performing Installation Tasks screen is displayed.
6. The Installation Complete screen is displayed after the software is installed. Click **Finish** to exit the Setup Wizard.

After the installation is complete, see the Online Help (available from the Controller) and the section for administering EdgeSight for Load Testing for information about configuring Servers, Controllers, and Launchers.

To Install the Web Interface Support Components

The EdgeSight Web Interface Support software is installed on target systems running Web Interface 4.5 or higher. The software allows EdgeSight for Load Testing software to access applications that are available through the Web Interface.

To install the Web Interface Support software:

1. If you are installing from media, insert the media. Click on **Web Interface Support Installation**. If you are installing directly from the MSI file, double click the EdgeSight Web Interface Support MSI file to start the setup wizard. The Welcome screen is displayed.
2. Click **Next** to continue. The License Agreement screen is displayed.
3. After reading the license, select **I accept** and click **Next**. The User Info screen is displayed.
4. Enter the username and password for the user to be added to the EdgeSightWISecurity group. If you are performing the installation using a local machine account, enter the computer name and username (computername\username). If you are performing the installation using a domain account, enter the domain name and username (domainname\username).
5. Click **Validate** to validate the credentials. After the credentials are validated, click **Next** to continue. The Website Selection screen is displayed.
6. Select the Website where you want to install the application page. Click **Next**. The Ready to Install screen is displayed.
7. Click **Install** to start the installation.
8. The Installation Complete screen is displayed after the software is installed. Click **Finish** to exit the **Setup Wizard**.

Upgrading EdgeSight for Load Testing Components

Important: Upgrading EdgeSight for Load Testing from a Beta or Technology Preview release is not supported. You must first uninstall the early release version of the software and then install the released version of the EdgeSight for Load Testing software.

You can directly upgrade to the current version of the software from EdgeSight for Load Testing 3.0 or later. Tests developed on EdgeSight for Load Testing 2.7 or later can be used with this release.

Removing the Web Interface Components

After uninstalling the Web Interface components from a target system, some artifacts must be removed manually. In particular, the EdgeSightWISecurity group and the Application page (for example, Citrix/AccessPlatform/ site/eswi.aspx) are not automatically removed.

Administer

EdgeSight for Load Testing is an automated load and performance testing solution for Citrix XenApp and XenDesktop environments. The product extends the application performance visibility that these environments provide by introducing pre-production application performance tools. The following figure shows the EdgeSight for Load Testing components.

The Controller is used to record and create virtual user scripts and define tests. When the test is ready for playback, the Controller instructs the Launchers to run the test with a certain number of virtual users for a certain period of time.

The Launchers receive the commands from the Controller and generate virtual user ICA sessions on the target XenApp or XenDesktop systems. The number of Launchers required will vary based on the target virtual user load.

The Launchers then report session information back to the Controller for run-time and post run-time analysis.

This load generating software solution enables administrators to predict how systems will cope with high levels of user load. By simulating hundreds of virtual users and monitoring the responsiveness of the system under test, it allows the administrator to determine how the current configuration and hardware infrastructure will support anticipated demand.

Initial Configuration

The initial configuration describes the minimum configuration steps required to start developing scripts with the EdgeSight for Load Testing software. Additional configuration steps are required when you run load tests and are described in [Running a Load Test](#). The topics described are:

- [Configure Servers](#)
- [Configure XenDesktop Environment](#)
- [Configure Launchers](#)
- [Configure Controller](#)

Configure Servers

The servers that load tests will be applied to require the following software and user account settings:

- Presentation Server 3 or later or XenApp must be installed on the servers.
- A user account must be created that allows the test users to log into the system. A single account can be configured so that multiple users log in to the same account simultaneously. See [Setting User Session Limit](#).

Note: For a complete list of the hardware and software requirements, see the *Citrix EdgeSight for Load Testing Installation Guide*.

The following sections describe connection settings that are required on servers:

- [Ending Sessions Automatically](#)
- [Setting User Session Limit](#)
- [Setting Published Applications Settings](#)
- [Setting Seamless Logins](#)

Ending Sessions Automatically

During load testing, when virtual users disconnect from servers they must not leave remnant disconnected sessions. To ensure this, you must configure all servers to terminate when session limit is reached or the connection is broken:

1. Go to **Start Menu > Administrative Tools > Terminal Services Configuration Tool**.
2. Click on the **Connections** folder, and right click on the **ICA-tcp** connection.
3. In the resulting dialog, select **Sessions > Properties**.
4. For **When session limit is reached or connection is broken**, select **End session and Override user settings**.

Setting User Session Limit

If you are using Windows Server 2003 or later, the **Restrict each user to one session** setting must be disabled. Disabling this setting allows EdgeSight for Load Testing to use multiple copies of the same user.

1. Go to **Start Menu > Administrative Tools > Terminal Services Configuration**.
2. Click on the **Server Settings** folder, and right click on **Restrict each user to one session**.
3. In the resulting dialog, disable **Restrict each user to one session**.

Setting Published Applications Settings

If you connect directly to a server (without using an ICA file), you must configure the server so that any user can run non-published applications.

1. Go to **Start Menu > Administrative Tools > Terminal Services Configuration Tool**.
2. Click on the **Connections** folder, and right click on the **ICA-tcp connection**.
3. Select the **ICA Settings** tab
4. Disable **Non-administrators only launch published applications**.

Setting Seamless Logins

Although not a requirement, the recommended setup is to use EdgeSight for Load Testing with seamless user logins. This ensures that virtual users log in without human intervention.

1. Go to **Start Menu > Administrative Tools > Terminal Services Configuration Tool**.
2. Click on the **Connections** folder, and right click on the **ICA-tcp connection**.
3. In the resulting dialog, select **Login Settings**.
4. Select **Use Client-provided logon information**.
5. Unselect **Always prompt for password**.

Configure XenDesktop Environment

If you are load testing XenDesktop systems, you should disable client drive mapping using an HDX user policy. When the Auto connect client drives setting is disabled via the Citrix Desktop Studio, the prompt to allow drive mapping access is not displayed and does not interfere with load testing.

Configure Launchers

Launchers, the systems that load test users are started from, require the following:

- ICA Client - Version 8.1 or later of the ICA Client software is required to run load tests.
- Ports - Launchers use port 18747 to communicate with the Load Test controller.

The Launcher is installed as a service (Citrix EdgeSight Launcher Service). The service is set to start automatically.

In addition to these required settings, you may want to perform one of the optional configuration tasks.

Disabling System Beep

During load test execution, the system the launcher is installed on beeps each time a network connection is opened or closed.

Use the following command to temporarily disable the beep. When using this method, the beep is enabled when the system is rebooted.

1. Open a Windows command prompt screen. **Start > cmd**
2. Enter the following command: **net stop beep**

You can restart the beep service using the **net start beep** command.

Use the following command to permanently disable the beep:

1. From the Start menu, right click **My Computer > Manage**
2. Expand **System Tools** and select **Device Manager**.
3. From the **View** menu, select **Show hidden devices**.
4. Expand **Non-Plug and Play Drivers**.
5. Right click **Beep**, and select **Properties**.
6. Select the **Drivers** tab.
7. Click **Stop**. You can also change the Start-up type to Disabled so the beep service never starts.

Configure Controllers

This section describes configuration settings required on the system running the Controller prior to recording scripts.

The following ports are used by the Controller:

- Port 18747 must be available for the Controller to communicate with the Launcher
- Port 27000 must be available for the Controller to communicate with the License Server.

Configure License Server

EdgeSight for Load Testing uses Version 4.5 of the Citrix License Server. See the *Getting Started with Citrix Licensing Guide* for more information.

The License Server Configuration dialog identifies the host and port of the license server. Use the following procedure to identify the License Server for your system:

1. From the Main menu, select **Options > License Server Configuration**
2. In the **Connect to** field, enter the License Server name as an IP address or fully qualified domain name.
3. In the **Connect on port** field, enter the port the Load Test Controller uses to communicate with the License Server. The default port is 27000.

When a test is replayed, the EdgeSight for Load Testing software checks for the presence of a XenApp Platinum or Enterprise license on the specified license server. If a valid license is detected, you can run as many users as required.

If a XenApp Platinum or Enterprise license is not detected, the EdgeSight for Load Testing software checks for the presence of a XenDesktop Platinum or Enterprise license on the specified license server. If a valid license is detected, you can run as many users as required.

If you do not have a XenApp or XenDesktop Platinum or Enterprise license on the specified license server, but have Concurrent User (CCU) licenses, the number of users you can test with is limited by the amount for which you are licensed. When you start a load test, the number of CCU licenses that are checked out corresponds to the number of users you have created. If you create a load of five concurrent users, but created a total of 100 users, then 100 CCU licenses are checked out when you start the test.

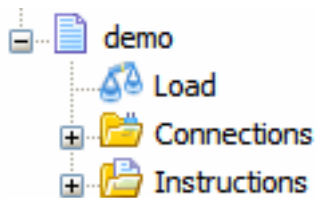
If no licenses of any kind are detected, the software displays the a message (Could not find a valid license on the designated license server) and offers to run in 15 user evaluation mode.

Create a Script

A script must be created as a placeholder for the instructions you record. A script requires a name, the size of the screen that displays test execution back to the Launcher, and an algorithm that defines how load tests are executed across multiple launchers.

When you create a script it contains three components:

- Load - defining the duration of a load test, the number of users that will execute the test, and how many users are concurrently executing the test.
- Connections - defining how the launchers connect to servers.
- Instructions - the discrete components of the test.



These components are organized in the Test Tree as shown in the following figure.

When you save a script, the Load and Connections information is saved with the instructions.

Use the following steps to create a script:

1. From the Menu bar, select **Test > Add Script**.
2. In the Script Properties dialog, enter a script name. There are no restrictions on the name that you use.
3. Enter the Client Size. The Client Size defines the size of the screen display for the session between the Launcher and the Server.

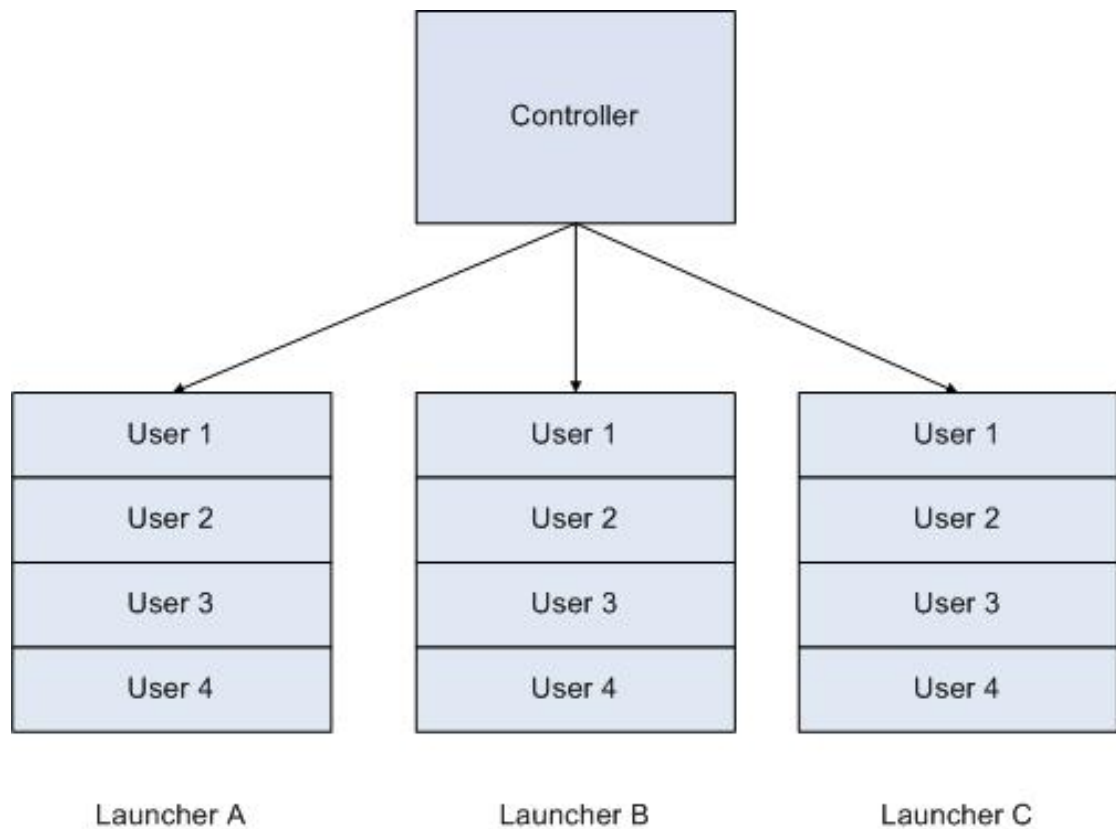
Note: If you record a script in one window resolution and then replay it in another resolution, the script may fail. Changing the screen size may cause mouse instructions to fail due to corresponding changes in X and Y window coordinates.

4. Select the algorithm for the Concurrency Model.

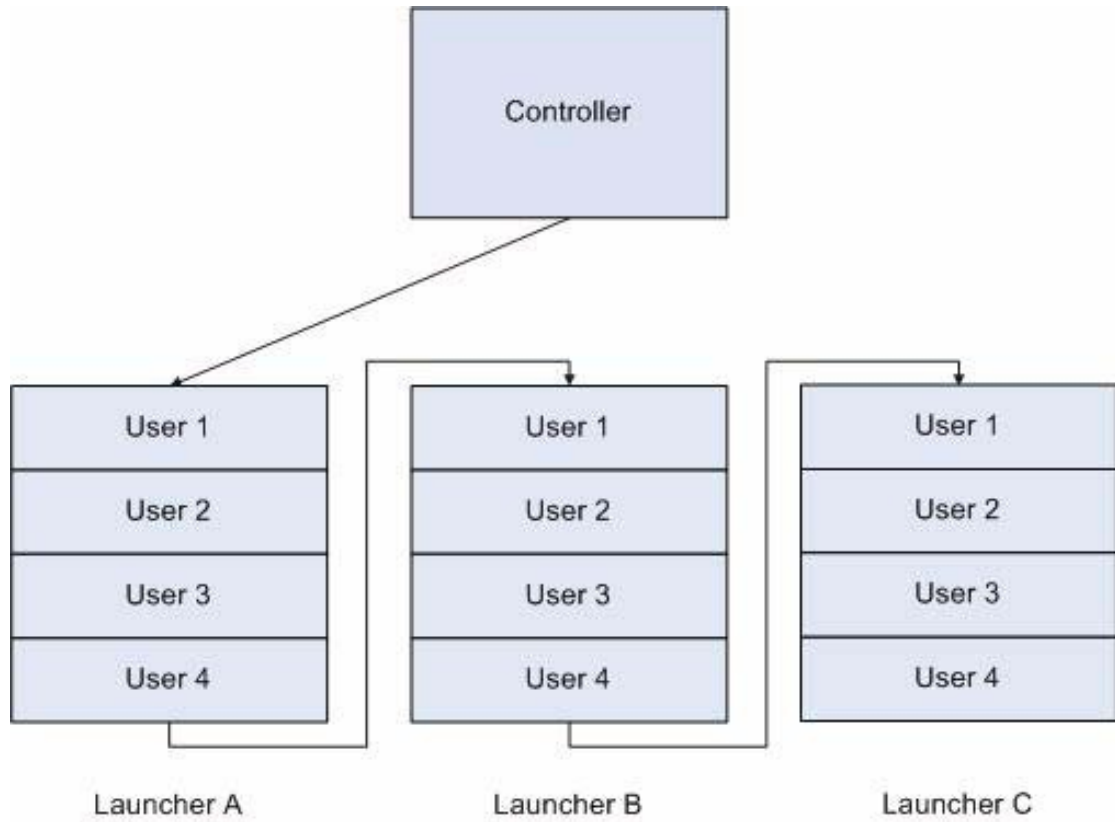
Concurrency Model

The concurrency model allows selection from three algorithms that specify the order tests are run when multiple launchers are used in a load test. The following figures illustrate the different concurrency models: Balanced, Rotated, and Top down.

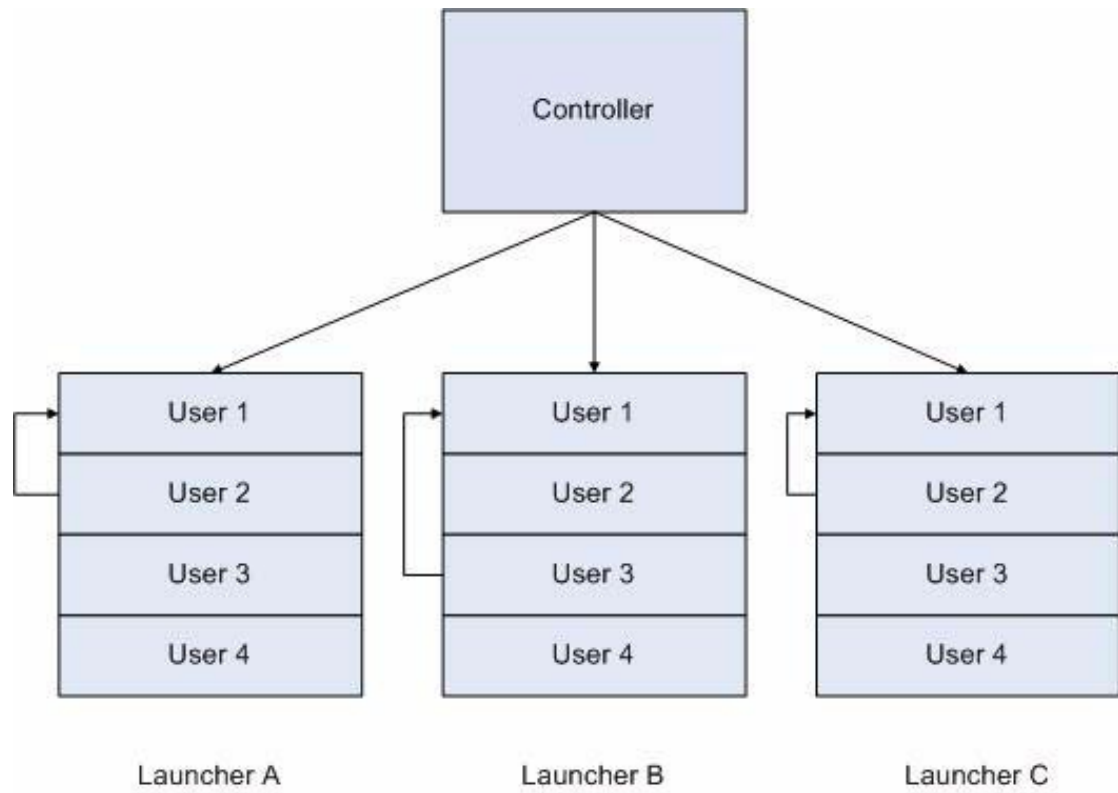
In the Balanced model, the controller directs an equal number of users on each launcher to execute tests.



In the Rotated model, the controller directs all users from Launcher A to run before the users on Launcher B start testing.



In the Top down model, the controller directs the first user in a launcher to execute the test whenever it is available to restart the test. In the following figure, Launcher A / User 1 is available to restart the test when User 2 completes the test. At the same time, Launcher B / User 1 is not available to restart the test until User 3 has completed testing.



Create a Connection

Connections define where users are launched from and the servers and applications to which they connect. A load test may have multiple connections defined. For example, a single load test may replicate a geographically dispersed Presentation Server or XenApp environment and require connections from three different locations.

Different types of connections are supported. Each launcher is limited to operating using a single type of connection during a load test. Connections can be made using the following methods:

- [ICA file](#)
- [XML Service](#)
- [Web Interface](#)
- [Server Desktop](#)

Connecting with an ICA File

EdgeSight for Load Testing can connect to published applications using ICA files.

You can create ICA files for published applications. The procedure for creating ICA files depends on the version of Presentation Server software you are running. See [Creating an ICA File](#).

Once you have an ICA file, you can use the following procedure to define it as the connection method:

1. Select the Connection node and click the **Add a Connection** button in the scripts toolbar. The Connection Properties dialog is displayed.
2. In the **Connect From** field, enter the address of the Launcher using an IP address or a fully qualified domain name.
3. Click **ICA file** and the **Browse** button to identify the ICA file. The ICA file identifies the Server and applications to connect to and is entered in the Connect To field.
4. To use the same ICA file for all Launchers, click the **Distribute** check box. This causes a copy of the ICA file to be sent to each Launcher.

Connecting with the XML Service

The XML service uses a Web Interface Connector to access published resources. Users log on to the Web Interface and see links to the applications that they are authorized to run.

Note: The Web Interface Connector is an optional feature that must be selected during the EdgeSight for Load Testing installation. If the feature was not installed, you can rerun the installation procedure to install it. To use the Web Interface Connector, you need the Microsoft Visual J# .NET Redistributable Package. See the *Citrix EdgeSight for Load Testing Installation Guide* for information about this requirement.

Use the following steps to connect using the XML service:

1. Select the Connection node and click the Add a Connection button in the scripts toolbar. The Connection Properties dialog is displayed.
2. In the Connect From field, enter the address of the Launcher.
3. Select XML Service and select the **Browse** button or enter the Server, port, and application in the Server field (server:port:application).
4. The XML Application browser is displayed. Enter the following fields:
 - a. Server Address and Port to connect to. The default port is 8080.
 - b. User Name, Password, and Domain of a valid user.
 - c. Select Search. The system displays available application.
 - d. Select the application you want to connect to.

Connecting with the Web Interface

The Web Interface allows you to access applications that are available through the XenApp or XenDesktop Web Interface. Before using this connection method, you must install Web Interface support using the EdgeSight Web Interface Support MSI file on the target system that you will be load testing. See the *Citrix EdgeSight for Load Testing Installation Guide* for more information.

- The installation places the Application Page (for example, Citrix/Accelerator/site/Swiss) on the Web Interface Server of the system you are load testing. You must correctly identify the location of the Application Page when configuring the Web interface.
- The installation creates the EdgeSightWISecurity group on the Web Interface Server. Users of the Controller and Launcher systems must be logged in with a user that is a member of this group. (Alternatively, you can specify Web interface access credentials as described in [Web Interface Access Credentials](#).)
- The Login Page differs depending on the target system. Depending on your configuration, you may need to change the default.

When you use the Web interface, the following authentication is performed:

1. Test users are authenticated against a list of users on the target system
2. The user logged on to the Controller or Launcher is authenticated, ensuring that they are a member of the EdgeSightWISecurity group. If configured, the Web Interface access credentials are used to authenticate the user.

Use the following steps to configure a connection using the Web Interface Application Browser:

1. Select the Connection node and click the Add a Connection button in the scripts toolbar. The Connection Properties dialog is displayed.
2. In the **Connect From** field, enter the address of the Launcher using an IP address or a fully qualified domain name.
3. Click the **Web Interface** radio button.
4. Click **Browse**. The system displays the Web Interface Application Browser dialog.
5. Enter the server address of the target system that you will load test.
6. Enter the Web interface login page you will be accessing. The default login page differs depending on the target system.
7. Enter the Application Page that contains the list of applications to be accessed by EdgeSight for Load Testing. Note that this page is loaded when the Web Interface Support MSI is run and is required to display applications in a format that is usable by EdgeSight for Load Testing.

8. Enter the Username, Password, and Domain of the valid EdgeSight for Load Testing user that will be logged in to the server during load testing.
9. Click **Search** to display the available applications.
10. Select the application to use and click **Select**.

If you have incorrectly configured the connection or if the Controller fails to authenticate with the Web Server, an error message will be displayed when you attempt to search for applications.

Web Interface Access Credentials

In order to successfully access the Web Interface, Controllers and Launchers must log in with an account that is a member of the EdgeSightWISecurity group on the Web Interface Server. If the account you are logged into is not a member of this group, you can use the Web Interface Access Credentials dialog to log in with the correct credentials.

Use the following steps to enter credentials for the Web Interface:

1. In the Connections Properties dialog box, click **Access**
2. Click the **Use the logged in users credentials** checkbox if the account you are logged into is a member of the EdgeSightWISecurity group OR Enter the Username, Password, and Domain of a user that is a member of the EdgeSightWISecurity group.
3. Click **OK**.

Connecting to the Server Desktop

Connecting to the Server desktop allows users to run applications available from the Desktop of the server.

1. Select the Connection node and click the Add a Connection button in the scripts toolbar. The Connection Properties dialog is displayed.
2. In the **Connect From** field, enter the address of the Launcher
3. Select **Server** and enter the Server address in the Connect To field.

When connecting to the Server Desktop, you must configure the server to allow users to run unpublished applications. See [Setting Published Applications Settings](#).

Create Users

Users are created for a specific connection. You must create a connection before creating users. See [Create a Connection](#) for instructions on creating a connection.

To create users, select a connection and then add the users for that connection. In order for users to successfully open connections to servers and execute load tests, they must have accounts and the proper credentials on the servers. See [User Accounts](#) for information about creating accounts on servers.

Use the following steps to create users:

1. Select the Connection for which you want to create users.
2. Select the Add Users to the Selected Connection button from the scripts toolbar.
3. In the Add Users to Connection dialog.
 - a. Enter the number of users you want to add.
 - b. Enter the number you want users to start at. Users are added as a single account (Tester). By numbering them, you can better identify each user (Tester1, Tester2....) in the Messages display. If a user times out during test execution, the specific user is identified. To enable this feature, you must click the check boxes next to the # character.
 - c. Enter the User name for the user.
 - d. Enter the Password for the user.
 - e. Enter the Domain name for the user.

View and Copy Users

You can view, edit, and copy users in the Main window. To view users, select the connection that the users are associated with. The users are displayed in the Main editing window.

You can copy users using cut and paste operations. If you have numbered the users, the numbers do not get incremented.

The user properties can be edited in the Main Editing window. You can change the user name, password, or the Domain for each user. To make changes to any of these fields, select the text in the field and edit the text. Use the Enter key to complete the changes.

Recording a Script

This chapter describes how to record a test, including starting, stopping, and restarting the recording. It also provides information that will be useful in developing strategies for creating scripts.

The topics described in this chapter include:

- [Strategy for Creating Good Scripts](#)
- [Starting a Recording](#)
- [Stopping a Recording](#)
- [Replaying a Recording](#)
- [Using Fast Record](#)

Strategy for Creating Good Scripts

In most cases, recording an entire script will be done in small increments. Larger scripts may require that you record parts of the script, debug and edit the script and replay it. When you have parts of the script that run error free, you add additional instructions to the script.

You can start or stop recording and add instructions at any point in the script. You can also replay selected portions of the script.

When you create large scripts, you can replay the scripts using the Fast Record option or JScript features to accelerate the replay.

Some of the practices that provide more reliable scripts include:

- Mouse instructions are usually the easiest way to record a script, but may be unreliable when running the load test. Replacing mouse instructions with keyboard instructions creates a more reliable test.
- Use folders to organize instructions. Group functional parts of the script into different folders. Use repeating and iterating folders to perform loops.
- Use wildcards in Synchronization Point captions. These allow you to identify screens with captions that change names. (For example, Microsoft Word Document 4, Microsoft Word Document 5....)
- Use Search and Match instructions for windows that cannot be identified because the window changes position or the text inside the window changes position.
- Don't save data to disk unless you require it as part of the test. Continuously saving data can cause storage problems, and saving and reopening files causes multiple dialog boxes to open and require response.
- Use the Messages screen to diagnose problems.
- Use Fast Record to reduce the time required to replay long scripts.
- Use Concurrency Control and Rate Control to avoid creating unrealistic network loads.
- Be aware of failures caused by exceeding timeout periods. Change the timeout periods for specific instructions.
- Use load control rules to automatically adjust test loads or change test formats when certain runtime conditions are met.

Starting a Recording

Prior to recording a script, you must configure the Servers, Controller and Launchers as described in [Initial Configuration](#).

When you create a recording, a single user must be selected to perform the instructions that are recorded. To select a recording user:

1. In the Test Tree pane, select **Connections** > **connection** (the connection that you created).
2. The list of users associated with this connection is displayed.
3. Select a recording user by clicking on the icon at the left of the user.

Start recording the test:

1. In the Test Tree pane, select **Instructions**
2. From the main toolbar, select the Record Test button













When the recording session starts, the following changes are visible:

- The Controller minimizes.
- A new window is created in the upper left hand corner of the screen.
- An ICA seamless host connection is made to the server.
- The Recording User is logged on.
- If you are connecting directly to a Server desktop, an ICA Seamless Host Agent dialog is displayed. You must click OK to continue.



Once you have acknowledged the ICA Seamless Host Agent dialog box, you begin recording instructions. Each mouse click, keyboard entry, and the windows that open during the recording session are recorded.

By starting a recording and then immediately logging out, you create a script that looks similar to the following. This is the simplest script you can create.

No.	Description
 2	ICA Seamless Host Agent
 3	31719
 4	Left Click
 5	Program Manager
 6	1406
 7	Left Click
 8	Start Menu
 9	1437
 10	Left Click
 11	Log Off Windows
 12	1547
 13	Left Click

Stopping a Recording

The recording session continues until you stop it, or log out of the ICA session. You stop the recording session using one of the following methods:

- Logging out of the ICA session, as shown in the script in the previous figure stops the recording process. When you exit the script by logging out you preserve all of the instructions that you have recorded in the script.
- From the main toolbar, select the Stop Test button to stop the recording and save the instructions that you have recorded. This may create a script that does not exit when you replay it. When you stop a script without logging out or closing the ICA session and want to record additional instructions, the script will replay to the point that it was stopped and then wait for additional instructions to be added.
- From the main toolbar, select the Cancel Test button to stop the recording and discard the instructions that have been recorded.

You can also use the **Test > Stop** and **Test > Cancel** menu items to stop the test.

Replaying a Recording

While you develop a script you may start, insert new instructions, stop, and replay the script multiple times. There are number of different ways to replay a script. Depending on the task you are trying to complete, use the following replay methods:

- To replay the entire recording, select Instructions in the Test Tree pane (the top level folder that you recorded the instructions under) and click the Replay Test button in the main toolbar. The recording replays all of the instructions that you previously recorded and stops at the last instruction. If the last instruction logs out of the ICA session, the recording session ends.
- To replay a recording so that it stops at a certain instruction, allowing you to record new instructions into the script, select the last instruction you want to execute and start the recording. The recording session plays back all of the existing instructions and stops at the selected instruction. At this point, you can add instructions to the script.

Using Fast Record

Fast record allows you to replay a script at more than twice the speed it normally takes to execute. This setting has no effect on the speed while you are running a load test. This is helpful when you are constantly replaying a script during editing or debugging.

Use the following steps to set the recording speed:

1. From the Main Menu, select **Options > Test Configuration**.
2. In the Test Configuration dialog, select the **Use fast record check box**.
3. Click **OK**.

Editing Scripts

Editing scripts allows you to change or tune the instructions that have been recorded. You can modify the properties of instructions, convert mouse instructions to keyboard instructions, add and delete instructions, and modify Synchronization Points using match and search features in the script.

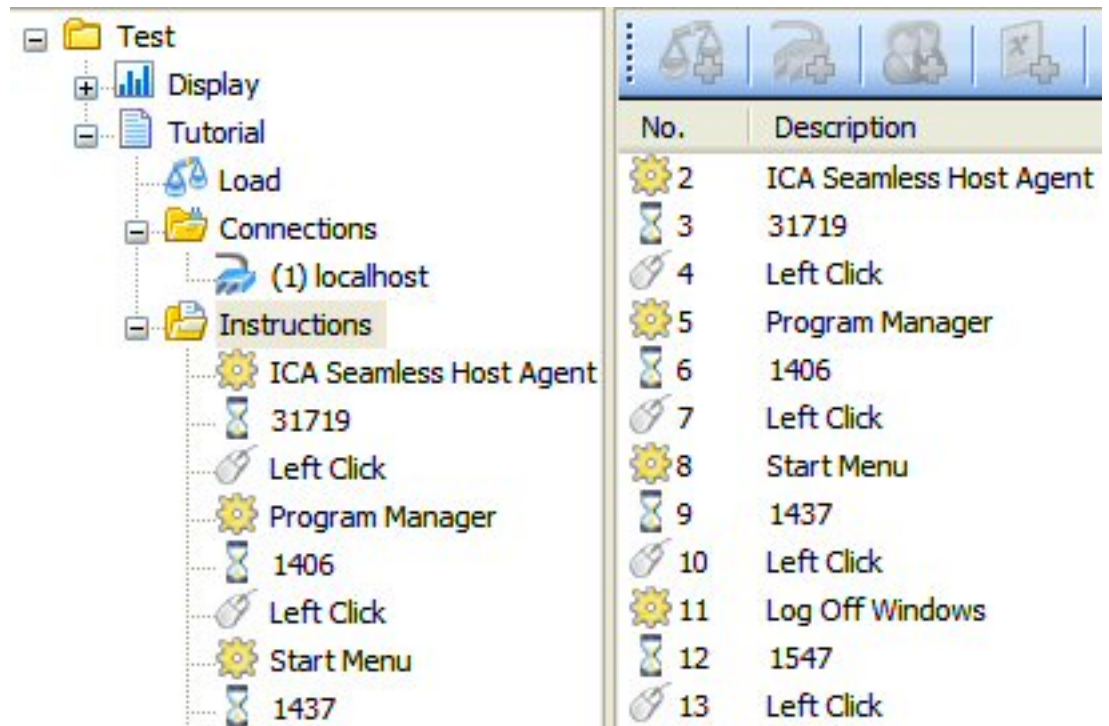
In most cases, the script development process requires repeated recording and editing sessions to create an acceptable script.

The topics covered in this section include:

- Navigation
- Folders
- Synchronization points
- Mouse input
- Keyboard input
- Variables
- JScript
- Comments
- Idle time






Introduction to Script Editing









After you record a script, you can customize the script by changing properties that control how each of the instructions of the script function. You can also add instructions that are not created during the recording session. Instruction that you add could include folders, variables, comments, JScript instructions, and idle time.



You can edit scripts in the Test Tree pane (left hand side), or in the Script Editing screen (right hand side). The following figure shows how scripts are displayed in each of these screens:

Each instruction type is identified by an icon:

-  The cog icon represents a Synchronization Point. Synchronization Points are instructions that cause a virtual user to wait for windows to appear or be in a predefined state before continuing. There are a number of settable properties for a synchronization point.
-  The hourglass icon represents idle time in the script. The idle time is recorded when you create a script. Idle time can be changed and you can add idle time between instructions in a script.
-  Folders can be used to organize multiple instructions. You can configure folders to repeat the instructions in them, to execute the instructions conditionally, or to not execute the instructions stored in the folder. There are a number of conditional folders:
 -  Iterating folders execute the instructions in the folder repeatedly until the controller determines that the user should log off.
 -  Repeating folders repeat the instructions in the folder based on a number of repetitions specified in the folder properties.

-  If Satisfied folders execute based on the success of a previous instruction.
-  If Not Satisfied folders executes based on the failure of a previous instruction.
-  Do Until Satisfied folders execute the contents of a folder until a designated instruction succeeds. The number of times to retry the folder is specified in the folder properties.
-  Do Until Not Satisfied folders execute the contents of a folder until it fails. The maximum number of times to retry the instruction is specified in the folder properties.
-  Do Not Execute folder never executes the instructions in the folder.
-  The keyboard icon represents keyboard instructions or a variable. Keyboard instructions include data entered into applications and keyboard commands.
-  The mouse icon represents mouse input. The input includes left and right clicks and mouse move operations.
-  The scriptlet icon represents an instruction that contains Microsoft JScript. The scriptlet allows you to execute custom JScript in a script.

Each instruction has settable properties. When you select an instruction in the Test Tree pane, the instruction properties are displayed and editable in the Main window. The following figure shows the properties for a Synchronization Point instruction.

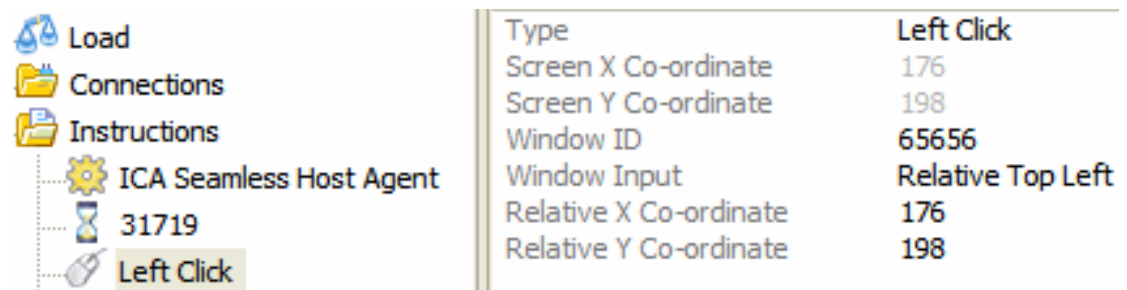
Synchronization Point	
Type	Exists
Caption	Program Manager
Style	Any
Bitmap Code	
ROI	232,354
Window ID	65632
Fail Mode	Logout
Timeout	30
Conditional Folder	None
Max Repeat	3

Navigation

Instructions are edited in the Test Tree pane and in the Main Window's editing pane. When you select the top level folder of instructions, all instructions are displayed in both the Test Tree and the Main Window.

In both the Test Tree pane and the Instruction Editing window, you can add, delete, and move instructions. You can also create folders and organize instructions into the folders.

When you select (click) an instruction in the Test Tree pane, the instructions properties are displayed in the Main Window.



The image shows a screenshot of a software interface. On the left is the 'Test Tree' pane, which is a hierarchical tree view. It contains several folders and items: 'Load' (with a blue icon), 'Connections' (with a yellow folder icon), 'Instructions' (with a yellow folder icon), 'ICA Seamless Host Agent' (with a yellow gear icon), '31719' (with a blue hourglass icon), and 'Left Click' (with a mouse icon). The 'Left Click' item is selected and highlighted with a light grey background. On the right is the 'Main Window' properties table, which displays the properties of the selected 'Left Click' instruction. The table has two columns: 'Type' and 'Value'. The 'Type' column lists various properties, and the 'Value' column shows the corresponding values for each property.

Type	Value
Screen X Co-ordinate	176
Screen Y Co-ordinate	198
Window ID	65656
Window Input	Relative Top Left
Relative X Co-ordinate	176
Relative Y Co-ordinate	198

You can change any of the settable properties in the Main Window. Select the property you want to edit and either select an option from a drop-down menu or edit the value with the keyboard.

Adding Instructions

There are a number of ways to add instructions to an existing script.

- Right-click the instruction you want to add an instruction above. From the drop-down menu, select the instruction you want to add.
- Select the instruction that you want to add the instruction above, then select the instruction type to add from the toolbar:



- In the Test Tree, select the top level folder of the script you are editing. Add instructions using one of the methods described previously. Instructions are added to the end of the script.
- In the Test Tree, select the folder you want to add an instruction into. Add an instruction to the bottom of any instructions in the folder using the menu or the toolbar. See “Moving Instructions” and “Using Folders” for more information on populating folders.

Moving Instructions

You may be required to move instructions after you have completed recording a script or when editing of the script. The majority of the time instructions are moved into folders.

In the Test Tree, you can drag and drop or cut and paste single instructions to perform moves within the Test Tree.

In the Main Window, you can select multiple instructions and drag and drop or cut and paste them into the Test Tree or within the Main Window.

- Each move operation results in the instructions being placed above the target instruction.
- When you move instructions into a folder, single instructions are added at the bottom of the folder, while multiple instructions preserve their order.
- Pasting an instruction on top of an instruction already in the folder places the new instruction above the original instruction.

Using Folders

Folders can be used to organize instructions, or to use the repeating or conditional features of the folder.

Use the following procedure to create and populate a folder:

1. In the Main Window, select the instruction that you want to create the folder above.
2. From the script toolbar, click the Add an Instructions Folder button.
3. Enter a name for the folder.
4. In the Main Window, select all of the instructions you want to move into the folder.
5. Drag and drop the instruction into the folder in the Test Tree pane.

Alternately, you can create a folder and move instructions into it in the Test Tree pane:

1. In the Main Window, select the instruction that you want to create the folder above.
2. From the script toolbar, click the Add an Instructions Folder button.
3. Enter a name for the folder.
4. In the Test Tree pane, drag and drop the instructions, one at a time, into the folder.
 - Dropping an instruction on top of the Folder places the instruction at the bottom of the folder
 - Dropping an instruction on top of an instruction already in the folder places the new instruction above the original instruction.

Note: You can create folders in the Test Tree pane, but a folder created on top of an existing folder is created as a sub-folder. When you create a folder on top of a folder in the Main Window, it is created above the existing folder.

Repeating Folders

In a repeating folder, the instructions in the folder execute until the specified repetitions are completed. If the execution time is longer than the time specified in the Load properties, the test continues until complete, overriding the time specified by the load. See [Creating a Load](#).

If the number of repetitions impacts the test duration specified by the load, an option to create a repeating test may be to use an Iterating Folder. See [Iterating Folders](#).

To configure a repeating folder:

1. Right click on the folder and select **Folder Properties**. The Folder Properties dialog is displayed.
2. From the **Execute** drop-down menu, select **Repeat**.
3. In the Max Repeat dialog, enter the number of times you want the folder to repeat.
4. Click **OK**.

Iterating Folders

Iterating folders are also repeating folders that continuously repeat the folder instructions until the Controller determines that the virtual user should log out.

Concurrency Control must be used with Iterating Folders to guarantee a certain numbers of users repeat the folder. Without setting concurrency control, the Controller will not execute the instructions contained in the folder.

Note: Rate Control is not required but is helpful for iterating tests. With rate control you can eliminate performance spikes caused by a large number of users starting testing at the same time. In addition, if multiple users fail or time out during the test, Rate Control prevents them from restarting tests simultaneously.

Using iterating folders ensures that the script tests the application rather than the ability of the server to service connections.

Use the following steps to create an Iterating folder:

1. Right click on the folder, select **Folder Properties**. The Folder Properties dialog is displayed.
2. In the **Execute** drop-down menu, select **Iterate**.
3. Click **OK**.

Set the Concurrency Control and the Rate Control for the folder using the following steps:

1. In the Test Tree pane, select **Load**.
2. In the Main Window, double-click the load that you want to modify.
3. In the Load Properties dialog, check the **Concurrency Control** box.
4. Enter the number of concurrent users you want running the test at start time and at completion time.
5. Check the **Rate Control** box and enter entry and exit rates.

See [Creating a Load](#) for information about Rate Control and Concurrency Control.

Conditional Folders

Conditional folders execute folders based on a previous instruction passing or failing execution. There are a number of different conditional folders:

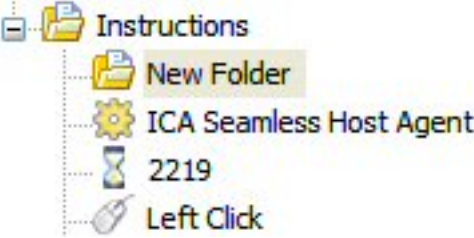
- If satisfied - execute the instructions in the folder if the specified instruction completed successfully.
- If not satisfied - execute the instructions in the folder if the specified instruction failed.
- Do until satisfied - execute the specified instruction until it is successful. The number of times to retry the execution is specified by the number specified in the Max Repeat field.
- Do until not satisfied - execute the specified instruction until it fails. The number of times to retry the execution is specified by the number specified in the Max Repeat field.

You can configure a conditional folder so that when it fails, execution of the script continues or the script exits with an error message.

Do Until Satisfied Example

Occasionally, when you click on OK in an ICA Seamless Host Agent dialog box to acknowledge the start of the session, the click is not recognized. An additional click must be entered to continue with the script.

To make certain that the mouse click is recognized, you can use a Do Until Satisfied conditional folder and enter the mouse click multiple times. The following steps describe how you configure the folder:

- 1. Create a folder above the first instruction in the script:

2219
2. Move the first three instructions into the new folder.
3. Modify the Folder Properties, selecting Do Until Satisfied for the Execute property. In the Max Repeat field, enter 3.

When the script starts, the instructions in the folder are repeated until the mouse click is recognized.

Creating Conditional Folders

To create a conditional folder, perform the following steps:

1. Create a folder (see [Using Folders](#)).
2. Right-click the new folder and select **Folder Properties**.
3. In the Folder Properties dialog:
 - a. From the **Execute** menu, select the type of condition to create
 - b. In the Synch No. field enter the number of the instruction that you are basing the condition on.
 - c. In the Max Repeat field, enter the number of times to repeat the instruction before the loop fails (for Do Until Satisfied and Do Until Not Satisfied conditions).

Folder Properties

Folder properties define how the instructions in a folder are executed. There are three properties that can be set when configuring a folder:

- Execute - defines the type of operation the folder executes.
- Synch No - identifies an instruction that a conditional folder is based on.
- Max Repeat - defines how many repetitions are performed.

The following table describes the Execute properties and notes which require Synch No. and Max Repeat properties.

Execute	Description	Requires...
Always	Execute the instructions in the folder	N/A
Iterate	Instructions in the folder are repeated continuously during the load test. The controller determines when the instructions exit the loop and log out of the test. Concurrency control must be used with iterating folders.	N/A
Repeat	Instructions in the folder are repeated the number of times specified in Max Repeat.	Max Repeat
If Satisfied	Instructions in the folder are executed if the Synchronization Point is satisfied.	Synch No
If Not Satisfied	Instructions in the folder are executed if the Synchronization Point fails.	Synch No
Do Until Satisfied	The instructions will be repeatedly run until the Max Repeat value is reached or the Synchronization Point is satisfied.	Synch No, Max Repeat
Do Until Not Satisfied	The instructions will be repeatedly run until the Max Repeat value is reached or the identified Synchronization Point fails.	Synch No, Max Repeat
Never	The instructions in the folder are not executed. This is useful for temporarily suspending execution when creating or debugging a script.	N/A

Synchronization Points

Synchronization Point instructions cause virtual users to wait for an application window to be in a defined state. Once correctly defined, instructions are executed in the window. When the specified event does not occur in the specified timeout period, the instruction fails and a timeout error is generated.

The following tables provide a description of the Synchronization Point properties. The Type properties identify how the Synchronization Point is identified before input is applied. For Match and Search synchronization points, you must specify bitmap recording options. You can also specify the suppression of mouse input. Mouse input can alter the graphical state of a screen, making it difficult to match a screen graphically.

Type Property	Description
Exists	Input synchronization is based on the screen existing. This is the default.
Does not exist	Input synchronization is based on the screen not existing.
Foreground	Waits for the window to be in the foreground.
Matches	A bitmap recorded synchronization point. The bitmap image is used to match the Synchronization Point that is always in the same position.
Does not match	Waits for the specified window's graphics around a point to not match the specified bitmap code.
Changed	Waits for the specified window's graphics to have changed since the last Synchronization Point. If a Bitmap code is specified then this instruction waits for a graphics change in the 10x10 pixel area in the window specified by ROI. If the ROI field is left empty then this instruction waits for any change in graphics in the entire window.
Search	A bitmap recorded synchronization point. During execution, a scan of the whole window is made to find the bitmap.

Style properties specify the style of the window to be matched. These properties are useful for differentiating between two windows with the same caption.

Style Property	Description
Any	Any style window or window property is accepted.
Menu	A window menu.
Dialog	A dialog box.
Child	The child window.
Maximized	A maximized window.
Minimized	A minimized window.
Significant	The window is of significant size.
None	No window style is specified.

The following table describes the remaining Synchronization Point properties.

Synchronization Points

Property	Description
Caption	The window caption that virtual users wait for before proceeding with the script. You can edit this field. The caption appears when you view the script in the Test Tree pane and the script editing screen.
Bitmap Code	For search and match synchronization points, a code derived from a 10 x10 bitmap screen capture.
ROI	Region of Interest. Used with match synchronization. Contains the point in the window at which the match bitmap was captured.
Window ID	The ID of the window. Used by mouse instructions to deliver input to the correct window.
Fail Mode	Describes whether instruction execution continues when this instruction fails.
Timeout period	The default is 30. The default can be changed in the Test Configuration dialog (Options > Test Configuration).
Conditional folder	The type of conditional execution the Synchronization Point performs. (See Conditional Folders).
Max repeat	For Do Until Satisfied and Do Until Not Satisfied conditional Synchronization Points.

Match Synchronization Points

Match synchronization points cause virtual users to wait for windows to be in a particular graphical state. When recording a match type synchronization point, a 10 x 10 pixel graphic image is captured in the area where the mouse clicks are applied. When virtual users execute a match type synchronization point, they compare the 10 x 10 pixel graphic image with the recorded image. The comparison is done at the same point, the ROI. If no match is found, the instruction fails.

Normally, you would use a Match Synchronization Point to replace a Synchronization Point that requires better detection of when the window is in the correct state for the script to proceed. Match Synchronization Points are useful for ensuring that a window is fully rendered on the screen before proceeding.

If you need to check for a graphical image that is not always in the same point in a window, use a Search Synchronization Point instead of a Match Synchronization Point. (See [Search Synchronization Points](#)).

To create a match synchronization point, use the following steps:

1. From the Main Menu, select **Options > Test Configuration**.
2. In the Test Configuration dialog, select the **Match** and **Suppress Mouse Move** checkboxes.
3. Click **OK**.
4. Restart the script, stopping it at the point where you want to add the Match Synchronization Point.
5. Add the Match Synchronization Point.
6. Stop the script.
7. Display the properties for the Match Synchronization Point you just created.
8. Change the **Type** property to **Matches**
9. Replay the script, the Synchronization Point instruction should be successful.

You should reset the Test Configuration options if you intend to add additional Synchronization Points to your script. Failure to do so may cause problems with mouse input created while the Suppress Mouse Move option is set.

Search Synchronization Points

Search Synchronization Points cause virtual users to wait for windows to be in a particular graphical state. When recording a Search Synchronization Point, a 10 x 10 pixel graphic image is captured in the area where mouse clicks are applied. When virtual users execute a Search Synchronization Point, they compare the 10 x 10 pixel graphic image to the entire window. If no match is found, the instruction fails.

Search Synchronization Points are CPU and disk intensive and should only be used when required.

To create a search synchronization point, use the following steps:

1. From the Main Menu, select **Options > Test Configuration**.
2. In the Test Configuration dialog, select the **Search** and **Suppress Mouse Move** checkboxes.
3. Click **OK**.
4. Restart the script, stopping it at the point where you want to add the Search Synchronization Point.
5. Add the Search Synchronization Point.
6. Stop the script.
7. Display the properties for the Search Synchronization Point you created.
8. Change the Type property to Search.

Using Search Synchronization Points is a good way of finding GUI items that are prone to move, such as icons on desktops or menu items that are subject to changing position in the menu. They can also be combined with mouse instructions as a method of targeting mouse input to a particular graphic.

To use targeted mouse input, use the following steps:

1. Create a Search Synchronization Point as described previously.
2. Edit the Window Input properties of the mouse instruction for the Search Synchronization Point. Set the properties to On Search Point.

This directs the mouse input to the graphic that was searched for. If the window or menu moves, the mouse input moves to where the graphic was found during the search.

The mouse Window Input properties can also be set to On Relative Search Point for Search Synchronization Points. This allows you to apply input to an area relative to, or offset from the actual search point. This is useful when the search point is a menu item that requires input to an area not directly on the searched graphic. Creating a relative search point requires that you manually configure the Relative X Coordinate and the Relative Y

Coordinate properties.

Editing Keyboard Input

Keyboard instructions include text, commands, and references to variables. The variable can be a text variable or a variable defined in a scriptlet instruction. Variables are described in [Creating Variables](#) and [Using Microsoft JScript](#).

Keyboard input is defined by the Type, Modifier, and the keys that are entered. The following tables describe the keyboard properties.

Type	Description
Keys	Sends one or more characters. that can be a single character, multiple characters, or a virtual key.
Key down	Sends a key down. Can only be a single character.
Key up	Sends a key up. Can only be a single character.
Variable	Contains a variable name.

The Key down and Key up types are used in multiple-key input, such as CTRL+C

Key modifiers include:

Modifier	Description
Control	The Ctrl key is pressed.
Alt	The Alt key is pressed.
Ext	The Ext key is pressed.
None	No key modifier is applied.

The Keys field describes the input to the script:

Keys	Description
Text	The text is entered into the window and represents text, virtual keysa , or a combination of virtual keys and text.
Variable	A variable name is entered.

The list of virtual keys is provided in [Virtual Keys Reference](#).

Keyboard Examples

The following examples demonstrate use of keyboard input as commands in a script. These examples are of multiple key and single key commands.

Use the following keyboard input sequence to enter a Alt+F keyboard command (the hot key to the file menu in an application):

Keys	Type	Modifier
[VK_MENU]	Keys	None
f	Keys	None

For a CTRL+Alt+Del command entered using only virtual keys, use the following input:

Modifier	Type	Modifier
[VK_CTRL]	Key down	None
[VK_ALT]	Key down	None
[VK_DELETE]	Keys	None
[VK_ALT]	Key up	None
[VK_CTRL]	Key up	None

You can use the Microsoft Windows key in keyboard sequences. For example, to use the Windows key to open the Windows Run dialog box and start a WordPad session, use the following keyboard input:

Keys	Type	Modifier
[VK_LWIN]	Key down	None
R	Keys	None
[VK_LWIN]	Key up	None
wordpad	Keys	None
[VK_RETURN]	Keys	None

For many key commands, there is more than one way to enter the command. For example, to exit a WordPad session using keyboard commands, you would enter: Alt+F to access the File menu and the x key to exit the session. You can enter these commands using either of the two methods listed in the following table:

Keys	Type	Modifier
Method 1		
[VK_ALT]	Key down	None
f	Keys	None
[VK_ALT]	Key up	None
x	Keys	None

Keyboard Examples

Method 2		
f	Keys	Alt
x	Keys	None

Editing Mouse Input

The Mouse Instructions send mouse input to screen or window coordinates. Each instruction contains a type of mouse action, coordinates, and the ID of the window that the operation is taking place in.

Mouse instructions make recording scripts easy, but can be an unreliable input method when executing a test. Mouse instructions fail when windows or menus are repositioned, causing the mouse coordinates to be invalid. For example, if you create a script that opens a window by clicking on a Desktop icon, that icon may move when a file is added to the Desktop. If the icon moves, the mouse instruction fails because it is no longer clicking on a valid coordinate. The same is true if a menu item moves or if the position of a dialog box changes in an application.

In many cases, the instructions you created with mouse input can be replaced with keyboard input. For example the File, Exit mouse clicks can be replaced with the Alt, f, and x keys.

Mouse properties include the following:

Mouse Input	Description
Type	The type of mouse operation and can include left click, left down, left up, left double click, right click, right down, right up, right double click, middle click, middle down, middle up, and middle double click. Mouse up and down keys can be used in combination to simulate drag and drop. When you drag the mouse you normally use key down and Window coordinates and then key up and Screen coordinates.
Screen X coordinate	The X coordinate relative to the top left of the screen. Used when Window input is Relative top left.
Screen Y coordinate	The Y coordinate relative to the top left of the screen. Used when Window input is Relative top left.
Window ID	The ID of the window that the mouse input is sent to.
Window input	Identifies the method of window input: Relative top left - input is delivered to the X and Y coordinates relative to the top left of the window. If the window ID is 0, the screen coordinates are used. On search point - the mouse input is delivered to the coordinates where the graphic was found. Relative search point - the mouse input is delivered to coordinates relative to the point at which the graphic was found. Used to enter text into a text field at coordinates relative to a search point.
Relative X coordinate	The X coordinate relative to the window Used by relative top left and relative search types.

Relative Y coordinate

The Y coordinate relative to the window. Used by relative top left and relative search types.

Creating Variables






By default, all virtual users enter the same data throughout test execution. To create a more realistic test, you can use variables that allow each user to enter unique text into applications.

A User Variable is a data value specific to an individual virtual user that can be accessed from within the script. Multiple variables can be defined for each script so that simulated users can have access to an unlimited amount of 'individual' data.

Use the following steps to create a variable:

1. In the Test Tree pane, select **Connections** > **connection** to display the list of users for your test.
2. Right-click a user and select **Add Variable**. The systems displays the Add Variable dialog box.
3. Enter a Variable Name
4. Enter the variable text

In the Main Window, the variable is shown being applied at all users:

No.	Username	Password	Domain	VarTxt
 1	tester1	*****	mydomain	Add unique text
 2	tester2	*****	mydomain	Add unique text
 3	tester3	*****	mydomain	Add unique text
 4	tester4	*****	mydomain	Add unique text
 5	tester5	*****	mydomain	Add unique text

In this example, *VarTxt* is the variable name and *Add unique text* is the variable. You must edit each user's variable to create unique text:

1. Double-click the variable text you want to change.
2. Enter text and then press the Enter key to exit the editing session.

To use the variable in a script, add a keyboard instruction, setting the Type property to Variable and entering the variable name into the Keys field:

Note: You cannot enter a return key into the variable text you are editing. In addition, if you cut and paste text into the Variable text box, return keys (multiple paragraphs) are not recognized. You can separate paragraphs using the [VK_RETURN] virtual key. For more information about virtual keys, see [Virtual Keys Reference](#).

To delete a variable:

Creating Variables

1. Select the variable name in the Main Window.
2. Right-click on the selected text.
3. From the options dialog box, select Delete Variable.

Importing Variables

You can import variables using a variable file. A variable file can be a comma-separated text file or a CSV file and include multiple variables. The first line contains variable names and each subsequent line contains the variable values. The first line of variable values is applied to user number 1.

Variable names can contain a-z, A-Z, 0-9, and _ (underscore).

Variable values can contain any characters except for a comma (,). Commas can only be used as the field separator. An imported file with N/A as a variable value preserves existing values.

- *Variable1, Variable2, Variable3*
- *name1, address1, phone1*
- *name2, address2, phone2*
- *name3, address3, phone3*
- *name4, address4, phone4*

When you import variables, the variable names and the variable values are created for users. The number of users that variables are created for is limited by the number of lines in the file.

If the variable file contains less lines than there are users defined, variables are created for all users, but the variables created for the additional users contain empty value fields.

Note: When you import variables, if the a variable with the same name exists, the variable data is overwritten by the imported file.

Using Microsoft JScript

Scriptlet Instructions allow you to add snippets of Microsoft JScript programming language into scripts. You can then leverage variables within the scriptlet instructions in subsequent keyboard input instructions. In the Test Tree pane, the instructions are implemented as follows:

```
S 22 // MyVariable=Math.round(Math.random()*45);  
K 23 MyVariable
```

Scriptlets can be used to create variables, such as random numbers, that are entered by virtual users as part of a Keyboard Instruction. They can also be used to control the execution of scripts when conditional Synchronization Points and folders do not provide adequate coverage. For the scriptlet in the previous figure, the instruction properties are displayed in the following figures

Note: Invalid scriptlet instructions may cause scripts to execute incorrectly.

The keyboard Type is set to Variable and the name of the Variable is entered in the keys field.

The Scriptlet instruction properties contain the variable name and the JScript code.

Scriptlet	22
JScript	// MyVariable=Math.round(Math.random()*45);

Supported Built-in JScript

Available methods to call from Scriptlets include the following:

Scriptlet	Description
User.IsSatisfied(number instruction);	Returns true if the instruction was satisfied.
User.GetVariable(string variable name);	Returns the virtual users value for the specified variable name.
User.SetSpeed(number speed multiplier);	Multiplies the virtual users idle time and typing speed by the supplied value. For example, if speedMultiplier is set to 0.1 then the idle times will be one tenth of their original value.
User.GetRunCount();	Returns the number of times a virtual user has executed its script during a test.
User.Logout(Boolean error);	Forces a virtual user to logout. If error is set to true, then an error is generated with the error message supplied.

User.SetSpeed() Example

To speed up the execution of the script, or certain parts of the script, use the User.SetSpeed() scriptlet as shown following sample:

```
//User.SetSpeed (0.1);  
Text entered in Wordpad  
//User.SetSpeed (1.0);
```

- The User.SetSpeed(0.1) is used to set the input speed to ten times the default speed.
- Text is entered in the WordPad window at the increased speed.
- The User.SetSpeed(1.0) scriptlet is called to return the speed to the default value.

Running a Load Test

This section describes the steps required to start a load test. The topics described include:




- [Creating a Load](#)
- [Starting a Test](#)
- [Stopping a Test](#)
- [Scheduling Tests](#)

Creating a Load

The load defines the duration of the test and how many virtual users are running at the beginning of the test and at the end of the test. Optionally, you can specify the rate that users enter and exit the test and specify the number of users running when the test starts and the number of users running when the test completes.

Without using Rate or Concurrency options, users are added to the test in a linear fashion. That is, for a test running one hour with 100 users, you can expect 50 users to be running after one half hour.

You can create multiple loads for one test. When multiple loads are used, the test executes one load after the other. This allows you to run tests with different amounts of users. For example, if you wanted to simulate an environment that changes over a 24 hour period, where the users may change from 100 to 40 and then to 20, you can create a load similar to the following:

Duration (min)	Start Rate	End Rate	Start Users	End Users
 480	60	60	1	100
 480	60	60	10	40
 480	180	180	1	20

Concurrency Control

When the Concurrency check box is selected the system attempts to maintain a count of executing virtual users as specified by the At Start and At End fields. The target user count is ramped between the start and end values over the course of the load, in a linear fashion.

Rate Control

When the Rate check box is selected the system attempts to connect new virtual users at the rate specified by the Connection Interval fields for the load. This rate value represents the time (in seconds) to wait before connecting a new virtual user. Rate control reduces the network load created when multiple simultaneous connections to the server are made.

Rate Control determines not only how new users enter the test, but also control the rate that users attempt to reenter the test because of failure or timeout.

Add a Load

Use the following steps to configure the Load:

1. In the Test Tree pane, select Load and click the Add a Load to the Script button in the script toolbar. The Load Properties dialog box is displayed.
2. Enter the number of minutes that you want the test to run.
3. Click Concurrent if you want the users to run concurrently. If you do not enable this option, only a single user will execute the test at a time.
 - Enter the number of users you want running when the test starts.
 - Enter the number of user you want running when the test completes.
4. Click Rate and enter a rate at which you want the users to connect.
 - Enter the rate for users to enter in the beginning of the test.
 - Enter the rate for users to enter at the end of the test.

Adding Load Control Rules

You can enhance your script and implement intelligent load control by adding load control rules. A load control rule allows you to automatically adjust test loads or change test formats when certain runtime conditions are met. Each rule is associated with a specific part of a test, which must have an associated measurable value. For example, you can create a load control rule for a script, folder, instruction, or synchronization point. You can create multiple rules for a single entity.

For a sample load control rule and the resulting load test data, see [Intelligent Load Control Example](#).

Each rule includes the following types of information:

- **Name**—A name for the rule.
- **Condition**—The condition which triggers the application of the rule, and the condition which causes the rule to be reset. For example, a rule can be triggered when the login failure rate exceeds 15 per minute, and then reset when the failure rate falls below 5 per minute. Both the triggering and resetting of the rule can be dependent on the condition occurring for a specified amount of time.
- **Effect**—The actions to be taken when the rule is triggered. Actions include stopping the creation of new users until a specified amount of time has passed, until the user count drops to a specified level, or until all active rules have been reset. The action can also be to terminate the test.
- **Affected script(s)**—One or more scripts to which the rule is applied and the resulting action taken.
- **Additional parameters**—You can specify a lag time from the start of the test to when the rule conditions are tested. You can also set a limit for the number of times that the rule can be triggered during a test.

To create a load control rule

1. In the Test Tree pane, select **Display**.
2. Select the **Scripts** tab or the **Counters** tab.
3. Select the part of the test for which the rule will be created. This can be a script, folder, instruction, or synchronization point on the Scripts tab, or a Windows or Xen counter on the Counter tab.
4. Click the Add a Load Control Rule button in the display toolbar. The Load Control Rule dialog box is displayed.
5. Enter a name for the rule. Names should be unique and descriptive to allow you to easily distinguish rules when adding them to the display.
6. Specify the rule conditions:

- Specify when the rule is to be activated by entering a value and choosing whether activation occurs when the actual value matches or exceeds (> or >=) or matches or falls below (< or <=) the value you supply. For example, if you want to trigger the rule when the Login Fail Rate measurement exceeds 15 per minute, choose > and enter 15.
 - Specify when the rule is to be reset by entering a value and choosing whether resetting occurs when the actual value matches exceeds (> or >=) or matches or falls below (< or <=) the value you supply. For example, if you want to reset the rule when the Login Fail Rate measurement falls below 5 per minute, choose < and enter 5.
 - Click the **Require parameter consistently over/below threshold** checkbox and enter a value in seconds that the condition must exist before activation or resetting occur. It is recommended that you use this feature to avoid implementing rules in reaction to brief spikes in activity.
7. Specify the rule effect by choosing one of the following options:
- Terminate test—When the rule is activated, the test is stopped.
 - Prevent starting users for affected scripts until all active rules have been reset—When the rule is activated, new users are not started until all the active rules associated with the selected script(s) have been reset.
 - Prevent starting users until user count for each affected script drops below n %—When the rule is activated, new users are not started until the user count for the selected script(s) falls below a specified percentage of the number of users at the time the rule was activated.
 - Prevent starting users for the affected scripts for n seconds—When the rule is activated, new users are not started until the specified number of seconds has elapsed.
8. Select one or more test scripts and click **Add** to apply the rule.
9. Select additional parameters as required:
- Do not apply the rule for the first n seconds of the test—Setting this parameter allows the test script to get through any initialization phases without having the rule activated.
 - Reactivate the rule no more than n times—Setting this parameter allows you to limit the number of times a rule is activated for each running of the test script.
10. Click **OK** to complete rule creation.

Starting a Test

Once you have defined connections, users, loads, and (optionally) load control rules, you can start a load test. You cannot start a load test with more users than you are licensed for, nor can you start one with more users than you have defined.

To start the test, select the Test node in the Test Tree pane and click the Replay Test button on the main tool bar. When you replay or debug a test, the test status and the running time are displayed in the script toolbar. Status messages and times are displayed in the Message pane at the bottom of the main window.

Viewing the Test Windows

When you start a test, a window for each user in the test is opened. By default, all of the windows are opened in the upper left hand corner of the screen. The windows are stacked on top of each other, making only one window visible.

You can view all of the user windows by displaying the windows tiled horizontally or vertically. To enable this display:

1. In the Windows Task bar, right-click the **Citrix EdgeSight for Load Testing - TUser task**.
2. Select **Tile Horizontally** or **Tile Vertically** to display all of the test users.

This view of the test allows you to monitor the progress of the test by viewing each user.

Replaying a Test in Debug Mode

As you develop the test, you may find it useful to run the test in debug mode. This allows you to set break points within a script. and then step through the script, either step by step, or to the next breakpoint. As the script runs, the active step is highlighted.

Note: As you develop the test, you may find it useful to run the test in debug mode. This allows you to set break points within a script. and then step through the script, either step by step, or to the next breakpoint. As the script runs, the active step is highlighted.

To debug a test:

1. Identify the steps in the script that will be used as breakpoints. In the Test Tree, open the **Instructions** folder and right click on an instruction and select **Set Breakpoint** to set a breakpoint. (To clear a break point, right click the step again and select **Clear Breakpoint**.)
2. From the main toolbar, click the Debug Test button. The Recording User message box is displayed.
3. Click **OK** to use the selected user as the debugging user. The TUser window is displayed. As instructions are executed, they are highlighted in the Test Tree and the caption of the TUser window is updated. Test execution continues until a breakpoint is reached.
4. To continue execution, click the Continue Test Execution or the Step to the Next Instruction button. Continue causes the test to be executed to the next breakpoint and Step Next causes the next instruction to be executed.

You may find the following keyboard shortcuts helpful when debugging tests:

- F5 - Test Debug
- Shift+F5 - Debug Continue
- F9 - Set instruction breakpoint
- Shift + F9 - Clear instruction breakpoint
- F10 - Debug Step Next

Stopping a Test

You can stop a test using the Main Menu or the main tool bar. There are two modes you can use to stop a test, Stop and Cancel.

When you Stop a test, the controller allows the users that are running scripts to continue to completion. After the scripts are completed, the clients are shut down and the licenses are returned to the license server. This is the most orderly method for stopping a test. The test may take some time to stop, based on the size of the script that is being executed, but this is the recommended way to stop a test.

When you Cancel a test the controller terminates all scripts that are running, shuts down virtual user sessions, and returns the licenses to the license server. This method is not recommended.

Scheduling Tests

You can schedule tests to automatically run at a designated date and time. To schedule a test:

1. In the main toolbar, click the Schedule Test button. The Test Scheduler dialog box is displayed.
2. Enter the Date and Time you want the test to start. Click Schedule to add the test to a list of scheduled tests. You can add multiple test times to the schedule.
3. Select Start logs automatically to create a log file of this test. A log file must have been defined for the test previously. The file will not be created by the test scheduler.

You can remove scheduled test from the list by selecting a test and clicking the Remove button.

Displaying Test Results

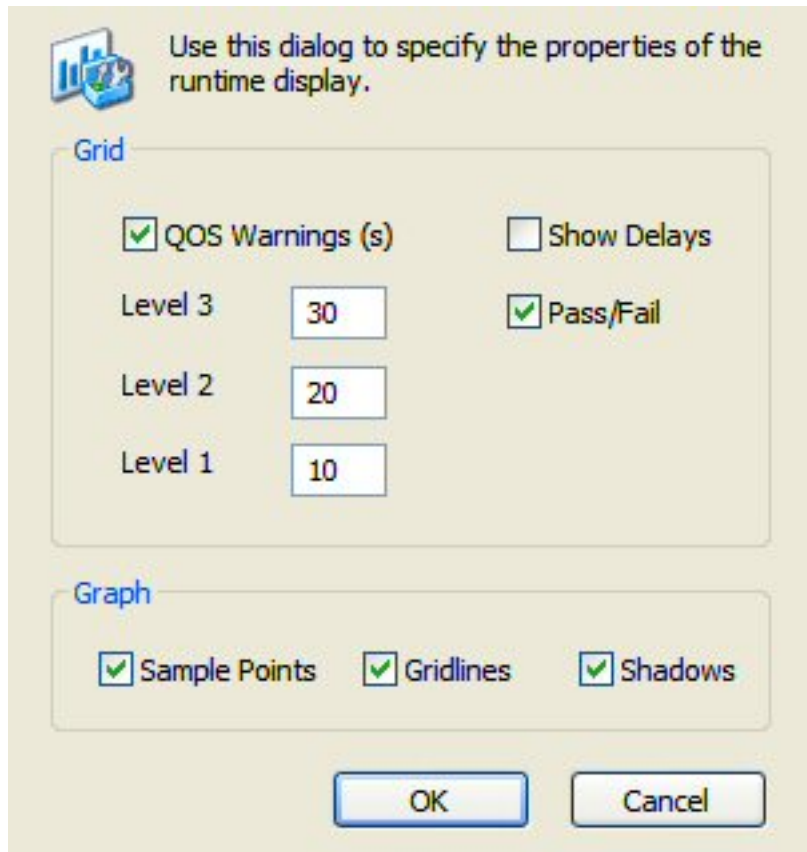
The display screens provide runtime information about the tests you are executing. The screens provide the following information:

- Scripts - provides an overview of the overall performance of the test you are executing and allows you to get more detailed performance information about certain parts of the test.
- Connections - displays performance statistics for each Launcher used in a test and displays statistics for specific instructions across each launcher.
- Counters - displays the counters that have been defined to measure the tests.
- Load Control Rules - displays the Load Control Rules which have been defined for the test.
- Alarms - displays alarms that have been triggered during test execution.
- Monitor - provides a graphical display of selected measurements.
- Measurements - provides a list of selected measurements that can be displayed in the Monitor screen. Used to add and remove instructions from the Display screen.
- Messages - displays messages generated during test execution.

Type	Script	Measurement	00:04:00		
	demo	Script	11	73.5	0

Display	Scale	Script	Measurement	Connection	Last
<input checked="" type="checkbox"/>	— 10	demo	Login Rate ...	All	0.0

To access the display screens, select Display in the Test Tree pane. The different screens are available by selecting the corresponding tabs in the Main window. A portion of the display is shown in the following figure.



You configure the display properties using the Display Properties dialog. To open this screen, right-click Display and select Properties.

Using the Display Properties dialog box you can configure the measurements that are displayed and the format of the Monitor screen.

Quality of Service (QOS) levels are used to visually indicate where system stress is causing delays in the executing scripts.

The QOS levels are delays measured against the average time an instruction takes to execute. The QOS levels are configured to highlight measurements when the preset performance levels are exceeded. The default settings for the QOS levels are:

- Level 3 - 30 seconds
- Level 2 - 20 seconds
- Level 1 - 10 seconds








Warning levels are displayed on the Scripts Window. Measurements exceeding the QOS levels are displayed in colors: Red (level 3), Orange (level 2), and Yellow (level 1).

Connect	41	2.1 (1.1)	0	65	2.5 (1.5)	0	39	7.4 (6.4)	0
Instructions (1)	34	30.1 (0.9)	0	63	30.3 (1.0)	0	48	33.7 (4.4)	0
Disconnect	34	1.7 (0.9)	0	62	1.9 (1.0)	0	49	3.8 (2.9)	0

Displaying Script Performance

The Scripts display reports the performance of the test as a whole. Performance statistics for the following are provided:

- User count - reports the average number of users currently executing the script.
- Connections - reports the average time required for each user to connect to the server.
- Disconnections - reports the average time required for a user to disconnect from the server.
- ICA Ping - reports the number of ICA Pings performed. High rates of ICA Pings may be an indication of connection problems between the users and the server.
- Script - displays performance of the currently defined scripts. Each script can be selected to display performance of individual instructions.
- Login Rate (/min) - displays the number of successful logins per minute.
- Login Fail Rate (/min) - displays the number of login failures and dropped connections per minute.

Type	Script	Measurement	00:04:00		
	demo	User Count	8		
	demo	Connect	24	4.2	0
	demo	Instructions (1)	15	65.1	1
	demo	Disconnect	14	10.3	0
	demo	ICA Ping (ms)	87		
	demo	Login Rate (/min)	20	5.0	
	demo	Login Fail Rate (/min)		0.0	0

For each measurement in the Scripts window, averaged performance data is shown in cells to the right of the measurement name.

Each data cell displays the following:

- The center value is the average response time for the selected measurement in seconds, or the average number of executing users in the case of a User Count measurement.
- A center value in parentheses indicates the average delay for users at this point in the script measured against the fastest execution.

Displaying Script Performance




- The value on the left indicates the number of virtual users that have successfully executed the measurement.
- The value of the right indicates the number of virtual users that have failed to execute the measurement.

The average delay, success, and failure values are optional and are set in the Display Properties dialog box.

As a test executes, the cells in the Scripts display are populated with data. The response time for each cell is averaged over the interval set for the cell. The default interval is two minutes. Pass and fail counts are totalled over the same interval.

You can change the start time and the interval length using the buttons on the script toolbar. Clicking the Move Left and Move Right buttons changes the start time and clicking the Zoom In and Zoom Out buttons changes the interval length.

Detailed performance information can be obtained for Script, Folder, and Synchronization Point measurements by drilling down on a measurement. Detailed performance information is provided for the immediate children of the measurement you select.

Type	Script	Measurement	00:04:00		
	demo	ICA Seamless Host ...	12	35.8	0
	demo	Program Manager (5)	12	0.0	0
	demo	Start Menu (8)	12	0.3	0

Instructions grouped together in a folder allow you to obtain performance data for specific transactions (the specific transactions inside the folder). Double-clicking on the Instructions cell results in a display similar to the following:




Connections Window

Use the Connections window to display the statistics for each connection to the sever or to displays the status of a single measurement across multiple connections.

Use the following method to display all of the connections in a test:

1. In the Test Tree pane, select **Display**.
2. In the main window, double-click the **Scripts** tab.
3. From the Scripts listing, select **Connect**.

4.

	Connection		00:02:00	
	(1) localhost	8	3.9	0
	(2) system2.my...	7	2.1	0
	(3) system3.my...	6	4.7	0

 Select the Connections tab. All of the connections statistics are displayed:

You can select a measurement from the Scripts Window and display the measurement for each connection in the test. This display allows you to compare the performance of the instruction across different connections.

To add instruction measurements to the Connection Window:

1. In the **Scripts** Window, select the measurement that you want to display across all connections.
2. Select the **Connections** tab. The measurement is displayed for all of the connections in the test. The name and number of the instruction is displayed as the title of the display.

You can add measurements from the Connections window to the Monitor window. This allows you to graphically compare the measurement across multiple connections. To add connections measurements to the Monitor window:

To add connections measurements to the Monitor window:

1. Right-click the measurement in the Connections window.
2. Select **Add Measurement** to Display.
3. In the Measurements window, select the check box next to the measurement.

Counters Window

Selecting the Counters tab displays the current averaged values of performance counters you have selected to monitor. The performance counters are ones selected for monitoring from the Microsoft Performance counters or from the Xen Server counters.

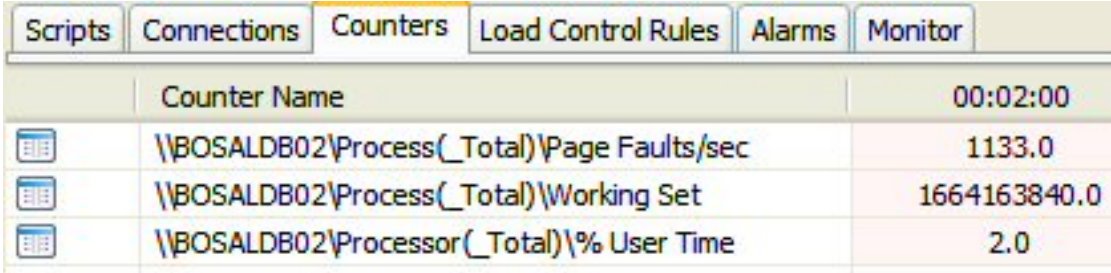
Add Windows Counter




Use the following steps to add Windows performance counters to the test. Performance counters cannot be added to a test that is running.

1. In the Test Tree pane, select **Display > Counters**.
2. From the display toolbar, select the **Add Windows Counters** button.
3. In the Select a Counter to Add screen, click the **Select Counters** from Computer button.
4. Enter the network address of the server under test.
5. Select the Performance Object field. A connection is created to the server you specified.
6. Select the counter to monitor.

Note: Each counter must be added individually, the Select All option does not work.

Note: Selecting a Counter Detail increases and decreases the number of counters available to select from. The Wizard level provides the greatest number of counters, while the Novice level provides the fewest counters.



	Counter Name	00:02:00
	\\BOSALDB02\Process(_Total)\Page Faults/sec	1133.0
	\\BOSALDB02\Process(_Total)\Working Set	1664163840.0
	\\BOSALDB02\Processor(_Total)\% User Time	2.0

Counters are displayed as follows:

Add Xen Counter

Use the following steps to add Xen performance counters to the test. Performance counters cannot be added to a test that is running.

1. In the Test Tree pane, select **Display > Counters**.
2. From the display toolbar, select the Add Xen Counters button.
3. In the Select Xen Server Counters screen, enter the IP address for the Xen pool master in the **Xen Pool Master's IP Address** field.
4. Edit the port number as required.
5. Enter a username and password used to access the Xen pool master.
6. Click **Query**. The **Xen Systems** list box is populated with the names of systems in the Xen pool. Both physical and virtual machines are displayed. Virtual machine names are indented under the associated physical machine.
7. Select a machine and then click the checkbox for each Xen counter to be collected for that machine. Continue selecting machines and counters as needed. As counters are added, they are displayed in the **Added Counters** list box. You can select one or more counters from the list and click **Remove** to delete the counter from the list, or click **Remove All** to delete all selected counters.
8. When you have finished selecting counters, click **Add**.

Delete Counter

You cannot delete a counter from the Counters display. Use the following procedure to delete counters.

1. In the Test Tree pane, select **Display > Counters**.
2. A list of counters is displayed in the Main window.
3. Select the counters you want to delete, right click on the selection and select **Delete**.

You can also delete all counters by right clicking in the Main windows and selecting **Clear All Windows Counters** or **Clear All Xen Counters**.

Load Control Rule Window

Use the Load Control Rules window to display the load control rules which have been enabled and displays the percentage of time that they were activated for each time period. (To enable or disable a rule, go to **Display > Load Control Rules**, right-click the rule, and select Enable/Disable.) For information on creating a load control rule, see [Adding Load Control Rules](#). For a sample load control rule and the resulting load test data, see [Intelligent Load Control Example](#).

Delete Load Control Rule

To delete load control rules.

1. In the Test Tree pane, select **Display > Load Control Rules** .
2. A list of rules is displayed in the Main window.
3. Select the rules you want to delete, or select multiple rules to be deleted.
4. Right-click the rule(s) and select **Delete**.

Alarms Window

You can add alarms that are triggered when a measurement you have specified reaches a certain value. The alarms can be used to generate records of performance events and can be configured to provide email notification of events.

To configure alarms, your test must already contain performance counters.

Selecting the Alarms tab displays the Alarms window. This window lists alarms that have been triggered during the current execution of the load test.

Add Alarm

Use the following steps to configure alarms:

1. In the Test Tree pane, select **Display > Counters** .
2. In the Main window, select the Counter Tab.
3. From the list of counters, select the counter that you want to add an alarm to, right click the selection, and select **Set Alarm**.
4. Enter the Alarm specifications in the Alarm Properties: New Alarm dialog box:

- a. Specify an alarm type:

Value alarms are triggered when the average value of a measurement reaches a specified level.

Pass Rate alarms are triggered when the pass rate (in percent) of the measurement reaches a specified percentage value.

- b. Specify if the alarm is triggered by a greater-than or less-than value.
- c. Specify an alarm trigger value.
- d. Choose a sampling interval.
- e. Choose a reset interval.
- f. Enter any comments which might help users understand the context of the alarm or appropriate actions.

To save the alarm to a file

1. Click the Write to File when triggered check box.
2. Enter the filename for the Alarm file.

To receive email notification of triggered alarms

1. Click the Send SMTP email when triggered check box.
2. Enter the email message specification.




Delete Alarm

Use the following steps to delete an alarm:

1. In the Test Tree pane, select **Display > Alarms**.
2. In the Main window, select the Alarm you want to delete, right click the selection, and select **Delete**.

Measurement Window

The Measurement window is positioned below the Display window, and is used to show summary data for selected measurements. From this display, measurements can be selected for display in the Monitor window.

Display	Scale	Script	Measurement
<input checked="" type="checkbox"/>  — 10	10	demo	Login Rate (/min)
<input checked="" type="checkbox"/>  — 10	10	demo	Login Fail Rate (/min)
<input type="checkbox"/>  — 100	100	demo	User Count

The measurements in this window can include Microsoft Performance counters, Xen Server counters, and counters selected from the Scripts display.

To add a measurement to the Measurement Console:

1. From the Scripts, Connections, Counters, or Load Control Rules window, select the measurement you want to add to the real time display.
2. From the display toolbar, select the Add a Monitor Measurement button.

The fields in the measurements display include the following:

- Display - contains an icon for the type of measurement, the color representing the measurement in the Monitor screen, and a check box to enable displaying the measurement in the Monitor screen.
- Scale - allows you to select a scale for the measurement in the Monitor screen.
- Script - identifies the script that the measurement is from.
- Measurement - identifies the measurement. An instruction contains an identification number.
- Connection - identifies the connection the measurement is from.
- Last - displays the most recent measurement.
- Max. - displays the highest measurement recorded.
- Min. - displays the lowest measurement recorded.

Monitor Window

The Monitor Window is used to plot the average values of selected test measurements against elapsed time. You can use it to examine the trends of multiple measurements simultaneously.

To view measurements in the graph view, you need to add it to the Measurement Console. Once added, click the check box alongside the measurement in the Measurement Console and then choose the Monitor tab. The average value of the measurement will be plotted on the graph against elapsed time.

You can change the start time and the interval length using Zoom Out and Zoom Into and the Move Left and Move Right buttons on the script toolbar. Clicking the Move Left and Move Right buttons changes the start time and clicking the Zoom Out and Zoom Into changes the interval length.

Messages Window

The Message Window displays status and error messages while tests execute. Messages displayed in this screen are cleared each time a test is started or restarted.

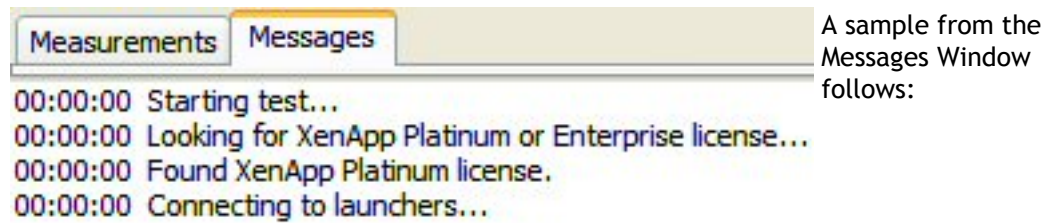


Chart Reports

You can view and save measurements displayed in the Monitor Window using the Chart Report function. Chart Reports are created as Microsoft Web Archive files (.mht) and saved in the default folder Citrix\Citrix EdgeSight for Load Testing\Reports. Each report includes the graphical data shown in the Monitor window, a list of measurement items and scales, and a table with the detailed measurement data.

To create a chart report:

1. In the Monitor Window, check the measurements you want to see in the report.
2. From the main toolbar, click the **Generate a Chart Report** button.
3. In the Chart Report Properties dialog, enter the Name of the chart report.
4. Enter a file name for the chart report in the Save As field.
5. If you want to save the chart report to a non-default location, click the **Browse** button and navigate to the selected folder. Click **Save** to save the new location.
6. Enter any comments you want included in the Chart Report.
7. Click **OK**.

Any measurements that you have highlighted are displayed in the Chart Display report. The resulting report includes the Monitor Window, the scale information for each measurement, and the data collected for each measurement.

Virtual Keys Reference

This Appendix describes the virtual keys supported as keyboard input. This information is provided as a supplement to the Keyboard Editing information in [Editing Keyboard Input](#).

The following table lists the supported virtual keys and describes the actual keys they support.

Virtual	Key
VK_NUMLOCK	Numbers lock
VK_SCROLL	Scroll
VK_BACK	Backspace
VK_TAB	Tab
VK_CLEAR	Clear
VK_RETURN	Return
VK_CONTROL	Ctrl
VK_MENU	Alt
VK_PAUSE	Pause
VK_CAPITOL	Caps Lock
VK_ESCAPE	Esc
VK_PRIOR	Page Up
VK_NEXT	Page Down
VK_END	End
VK_HOME	Home
VK_LEFT	Left Arrow
VK_UP	Up Arrow
VK_RIGHT	Right arrow
VK_DOWN	Down arrow
VK_SELECT	Select
VK_EXECUTE	Execute
VK_SNAPSHOT	Print Screen
VK_INSERT	Insert
VK_DELETE	Delete
VK_HELP	Help
VK_F1	F1
VK_F2	F2
VK_F3	F3

Virtual Keys Reference

VK_F4	F4
VK_F5	F5
VK_F6	F6
VK_F7	F7
VK_F8	F8
VK_F9	F9
VK_F10	F10
VK_F11	F11
VK_F12	F12
VK_F13	F13
VK_F14	F14
VK_F15	F15
VK_F16	F16
VK_F17	F17
VK_F18	F18
VK_F19	F19
VK_F20	F20
VK_F21	F21
VK_F22	F22
VK_F23	F23
VK_F24	F24
VK_LCONTROL	Left Ctrl
VK_RCONTROL	Right Ctrl
VK_LMENU	Left Alt
VK_RMENU	Right Alt
VK_SHIFT	Shift
VK_LWIN	Left Windows
VK_RWIN	Right Windows

Creating an ICA File

EdgeSight for Load Testing can connect to published applications and applications served through Web pages using ICA files.

You can create ICA files for published applications. The procedure for creating ICA files depends on the version of Presentation Server software you are running.

Note:

Creating ICA files using the following procedures may cause Load Tests to run with different default settings than those set on your system. These settings, which may include audio and window defaults, can be modified by editing the ICA files.

Creating ICA Files for Versions Prior to Presentation Server 4.5

Use the following steps to create an ICA file:

1. Open the Citrix Management Console and navigate to the published application you want to use.
2. Right click on the application you want to create an ICA file for.
3. Select Create ICA File.
4. Follow the steps presented by the Create ICA Wizard. By default, the ICA file is created in the Program Files\Citrix\Administration folder.
5. Copy the ICA file to the EdgeSight for Load Testing\ICA Files folder of the machine the Launcher(s) is running on.

When you create a Connection, use the ICA file you just created.

Creating ICA Files for Presentation Server 4.5 and Later

Use the following steps to create an ICA file on a Presentation Server version 4.5 System:

1. Launch the Internet Explorer Web browser and navigate to the Citrix Web Interface.
2. Log in to the Citrix Web Interface site.
3. Right-click the application that you want to create an ICA file for.
4. Select **Save Target As....**
5. Save the file to the EdgeSight for Load Testing\ICA Files folder.
6. Edit the file, deleting or commenting out the lines beginning with the following:
 - RemoveICAFile=
 - LogonTicket=
 - LogonTicketType=

Creating ICA Files from the APPSRV.ini File

You can use this procedure when using the XML service as a connection method.

Use the following steps to create an ICA file from the APPSRV.ini file:

1. From the **Start Menu**, select **All Programs > Citrix > Citrix Access Clients > Program Neighborhood**.
2. Double-click **Application Set Manager**.
3. Double-click **Custom ICA Connections**.
4. Double-click **Add ICA Connection**.
5. In the Add New ICA Connection wizard:
 - Enter the connection type.
 - Enter a description (Name), the network protocol, the server name, and the server desktop or the published application to connect to.
 - Select the encryption level.
 - Enter the Username, Password, and Domain for the account that will use the connection.
 - Enter the display settings.
 - Leave the Application and Working directory fields blank.
 - Click **Finish**.
6. Edit the C:\Documents and Settings*username*\Application Data\ICAClient\APPSRV file.
7. Search for the a line containing [ApplicationServers].
8. Delete the lines below this line except for the one containing the ICA name you entered in the Wizard, for example: [ApplicationServers] test2=
9. Write these lines to a new file.
10. Search for the name of the ICA you created with the Wizard. The name should appear as [name].
11. Select the [name] field and all lines below (before you encounter another [name] field).
12. Append these lines to the new file. The file should look similar to the following:

[ApplicationServers]

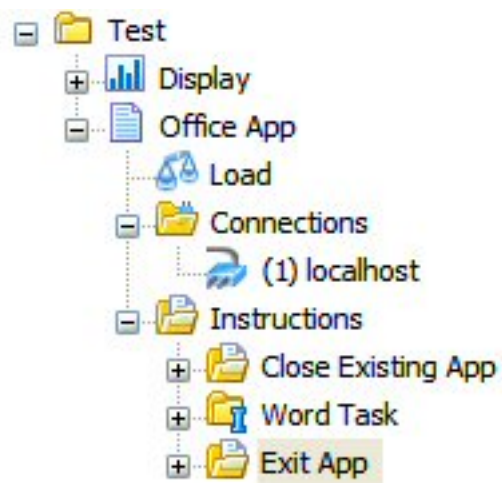
```
test2=  
[test2]  
TransportDriver=TCP/IP  
BrowserProtocol=HTTPonTCP  
DoNotUseDefaultCSL=Off  
Description=test2  
Address=tload01.qalab.local  
IconPath=C:\Program Files\Citrix\ICA Client\pn.exe  
.  
.  
.  
UseLocalUserAndPassword=Off  
DisableCtrlAltDel=On  
UIFlags=12  
SSLEnable=Off  
SSLNoCACerts=0  
SSLCiphers=ALL  
CGPAddress=*  
SSLProxyHost=*:443
```

13. Copy this file to the Citrix EdgeSight for Load Testing\ICA Files folder.

Script Example

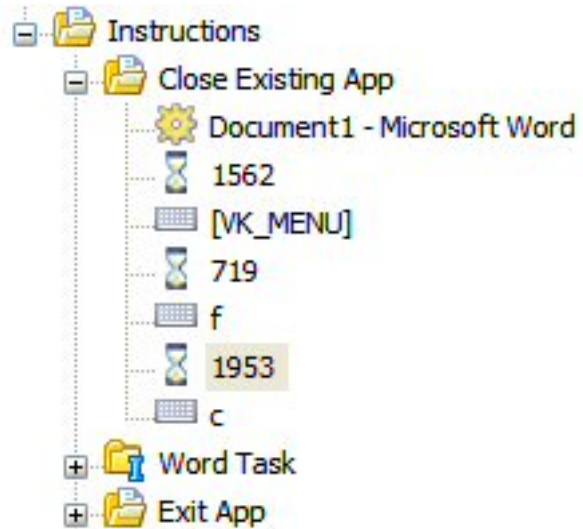
A simple script that demonstrates the use of some of the editing functions are:

- The script is organized into folders
- It uses an iterating folder
- Mouse instructions have been replaced by keyboard instructions
- Wildcards are used in the Microsoft Windows screen captions



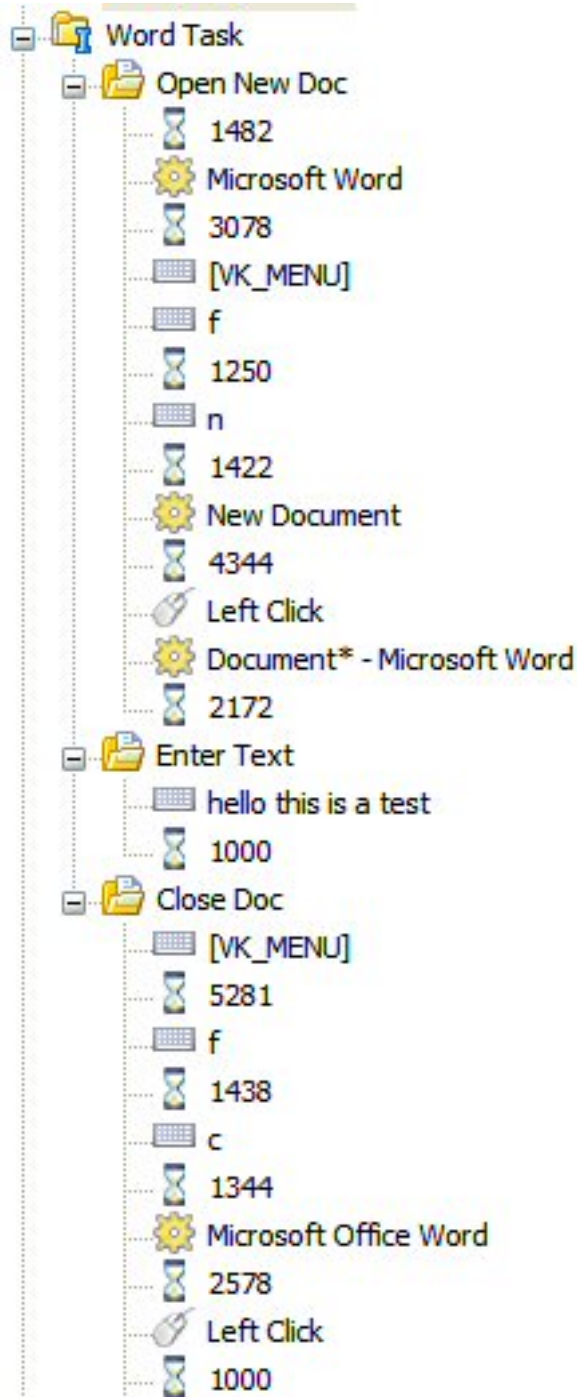
Without expanding the folders, the script is displayed in following figure.

Close Existing Doc Folder



The first folder of the script closes any file that is open when Microsoft Word starts. The File > Close mouse commands have been replaced with keyboard input.

Word Task Folder



The Word Task folder is an iterating folder and is organized with three sub folders. The iterating folder executes the instructions in the folder continuously, until the controller stops the iteration and exits the test.

Open New Doc Folder

In this folder, a new Microsoft Word document is opened. Because Microsoft Word uses captions with incremented titles (Documentn Microsoft Word), the caption for the Microsoft Word Synchronization Point uses a wildcard. This ensures that the caption always matches.

Enter Text Folder

The only instruction in this folder is the keyboard instruction that enters text into the Microsoft Word file.

Close Doc Folder

In this folder, the Microsoft Word file is closed without saving the file. A File > Close instruction is entered with keyboard instructions and a mouse instruction responds to the query to save the file.

Exit App Folder



The Exit App folder contains instructions that exit the Microsoft Word application and result in the connection to the server being closed. Note that the keyboard command is entered as a single command. In the Iterating folder, a similar keyboard command was entered as multiple commands.

Intelligent Load Control Example

The sample rule and chart report illustrates the usage and effect of a single, simple load control rule.

The intent of using load control rules is to allow the test to probe an area of interest in terms of system stress. Instead of a steady increase in user count which can stress the system beyond the point of producing meaningful data, intelligent load control allows EdgeSight for Load Testing to detect system stress and respond by reducing user count. This allows the system to recover to a point where the user count can start to increase again. This cycle of stress and adjustment produces repeatable and accurate data about system capacity.

Sample Load Control Rule

The following figure shows the sample load control rule parameters, including the following:

- When to activate and reset the rule. In this case, the rule is activated when the % disk time counter exceeds 90%, and is reset when the counter falls below 75%.
- A time period parameter required for rule activation. In this case, the rule is not activated until the % disk time counter exceeds 90% continuously for 90 seconds. This parameter helps prevent the rule from being triggered in response to transient spikes.
- The effect of the rule. All effects result in a reduction in user count. In this case, no new users are created until all active rules have been reset. (There can be multiple rules applied to a single script.)
- The script to which the rule will be applied. In this case, the Word Demo script is selected. The script has users open Microsoft Word, enter text, and close the application.

Load Control Rule

Rule Name

Specify Rule Condition

Activate Rule When
 > Value

Reset Rule When
 < Value

Require parameter consistently over/below threshold for the last seconds.

Specify Rule Effect

Terminate test.

Prevent starting users for affected scripts until all active rules have been reset.

Prevent starting users until user count for each affected script drops below %.

Prevent starting users for the affected scripts for seconds.

Test Script Selection

Available Scripts

Add >>

Remove <<

Scripts affected when rule triggers

Additional Parameters

Do not apply the rule for the first seconds of the test.

Reactivate the rule no more than times.

OK Cancel

The metric of percent (%) physical disk time was chosen because it is a known bottleneck for the particular script on the system under test. Other potential candidates for metrics are average disk queue, average CPU, memory, and network utilization.

When defining the load, the user concurrency should be chosen to rise at a rate which does not trigger the rule prematurely, creating unnecessary false positives and artificially prolonging the test duration. In this case, the load is defined as 120 users over a period of 15 minutes.

A good test will include a rule that triggers at a predictable rate, cycling up and down at an even level.

Sample Chart Report

Rule activation in relation to various metrics can be shown by adding the rule and desired metrics to the Monitor tab display. As seen in the chart report example below, the threshold values of the selected counters are in sync. As user count increases, disk time, disk queue length, and processor time also rise. After the load control rule is activated, the user count decreases, along with the selected metrics. This indicates that each metric would render the same result when used as a rule parameter.

The alternate and repeated effect of reducing the load when performance parameters are out of normal operating ranges, and then increasing the load when the parameters return within the normal operating ranges provides fast and accurate capacity determination for the tested system.

Load Test Chart Report

Report Name: LCR-Demo-PDT[90-75]-120u15m

File Name: C:\Documents and Settings\My Documents\Citrix EdgeSight for Load Testing\Reports\LCR-Demo-PDT[90-75]-120u15m.mht

Report Generated: May 13 2009 17:26:06

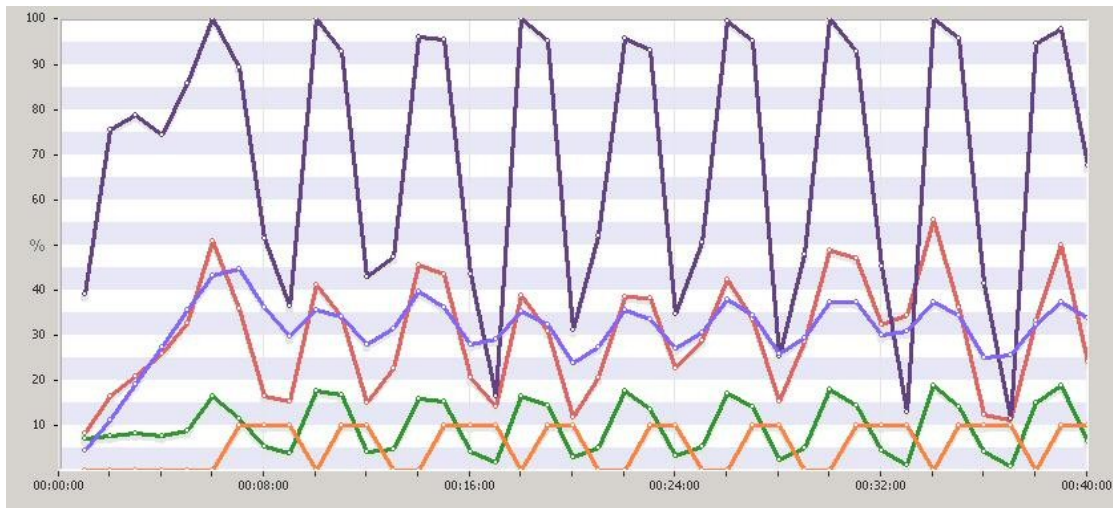


Chart itemscale

Item	Scale
% Disk Time - 90<->75 - All	10
Word Demo\User Count - All	100
\\eslt01\PhysicalDisk(_Total)\% Disk Time - All	100
\\eslt01\PhysicalDisk(_Total)\Avg. Disk Queue Length - All	10
\\eslt01\Processor(_Total)\% Processor Time - All	100

Comments: Load Control Rule Demo - Physical Disk Time [90-75] - 120 users over 15 minutes

Load Control Rule Runtime Activation Messages

The following represent runtime messages pertinent to rule activation.

00:00:00 Starting test...00:00:00 Looking for XenApp Platinum or Enterprise license...

00:00:00 Starting test...

00:00:00 Looking for XenApp Platinum or Enterprise license...

00:00:02 Found XenApp Platinum license.

00:00:02 Connecting to launchers...

00:00:03 Starting clients...

00:00:19 Executing test...

00:06:00 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 100.0.

00:08:30 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 37.6 25.4 27.1.

00:08:30 Rule % Disk Time - 90<->75 reset.

00:08:31 Load advanced 300 seconds, started 00:05:00, ends 00:20:00

00:10:01 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 100.0.

00:12:01 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 0.5 11.1 74.6.

00:12:01 Rule % Disk Time - 90<->75 reset.

00:12:01 Load advanced 210 seconds, started 00:08:30, ends 00:23:30

00:14:01 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 92.3.

00:16:31 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 0.4 5.2 8.3.

00:16:31 Rule % Disk Time - 90<->75 reset.

00:16:31 Load advanced 270 seconds, started 00:13:00, ends 00:28:00

00:18:03 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 100.0.

00:20:03 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 10.4 5.1 57.2.

Load Control Rule Runtime Activation Messages

00:20:03 Rule % Disk Time - 90<->75 reset.

00:20:04 Load advanced 243 seconds, started 00:17:03, ends 00:32:03

00:22:03 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 91.5.

00:24:03 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 0.3 4.0 65.4.

00:24:03 Rule % Disk Time - 90<->75 reset.

00:24:05 Load advanced 218 seconds, started 00:20:41, ends 00:35:41

00:26:04 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 99.0.

00:28:04 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 0.7 5.2 45.6.

00:28:04 Rule % Disk Time - 90<->75 reset.

00:28:05 Load advanced 248 seconds, started 00:24:49, ends 00:39:49

00:30:04 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 100.0.

00:32:34 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 0.4 6.4 13.2.

00:32:34 Rule % Disk Time - 90<->75 reset.

00:32:34 Load advanced 239 seconds, started 00:28:48, ends 00:43:48

00:34:04 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 100.0.

00:36:34 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 14.7 5.3 3.5.

00:36:34 Rule % Disk Time - 90<->75 reset.

00:36:34 Load advanced 278 seconds, started 00:33:26, ends 00:48:26

00:38:30 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 100.0.

00:40:01 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 58.3 66.9 68.1.

00:40:01 Rule % Disk Time - 90<->75 reset.

00:40:01 Load advanced 139 seconds, started 00:35:45, ends 00:50:45

00:42:01 Rule % Disk Time - 90<->75 activated, activation values are 100.0, 100.0, 91.2.

00:44:02 Rule % Disk Time - 90<->75 reset when parameter value = 75.0, current values = 0.2 2.8 67.3.

00:44:02 Rule % Disk Time - 90<->75 reset.

Load Control Rule Runtime Activation Messages

00:46:41 Shutting down clients...

00:46:43 Test stopped.