



Enterprise Chat and Email Design Guide, Release 11.5(1)

For Unified Contact Center Enterprise

August 2016

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Enterprise Chat and Email Design Guide: For Unified Contact Center Enterprise. November 17, 2016

Copyright © 2006–2016, Cisco Systems, Inc. All rights reserved.

Contents

Preface5

- About This Guide 6
- Obtaining Documentation and Submitting a Service Request 6
- Documentation Feedback 6
- Field Alerts and Field Notices 6
- Document Conventions 7
- Other Learning Resources 7
 - Online Help 7
 - Document Set 7

Chapter 1: Sizing Guidelines9

- Sizing Inputs 10
- Planning for Database Growth 10
- About Deploying on Virtual Servers 11
- Sizing for Combined Email, Web, and Voice Scenarios 11
 - Important Information About Sizing 11
 - Support for up to 400 Standardized Concurrent Agents 12
 - Support for 401 to 1500 Standardized Concurrent Agents 12
- Additional Configurations for Sizing 13
 - Changes on Web Servers 13
 - Updating Default Application Pool Settings 13
 - Updating Registry Settings 14
 - Updating ASP Settings 15
 - Updating the Worker.Properties File 16
 - Expanding the Disk Size on Database Server Machines 16

Chapter 2: Fault Tolerance and Redundancy18

- Load Balancing Considerations 19
- High Availability Options 20
- Managing Failover 20

Chapter 3: Network Latency	22
Network Latency.....	23
Bandwidth Requirements.....	23
Geographic Server Distribution.....	23
Chapter 4: Firewall and Hardening	24
Firewall Considerations.....	25
Server Hardening Considerations.....	25
Cisco Security Agent.....	25
Default Windows and IIS Service Requirements for ECE.....	26
Guidelines for Microsoft SQL Server.....	26

Preface

- ▶ [About This Guide](#)
- ▶ [Obtaining Documentation and Submitting a Service Request](#)
- ▶ [Documentation Feedback](#)
- ▶ [Field Alerts and Field Notices](#)
- ▶ [Document Conventions](#)
- ▶ [Other Learning Resources](#)

Welcome to the Enterprise Chat and Email (ECE) feature, which provides multichannel interaction software used by businesses all over the world as a core component to the Unified Contact Center Enterprise product line. ECE offers a unified suite of the industry's best applications for chat and email interaction management to enable a blended agent for handling of web chat, email and voice interactions.

About This Guide

Enterprise Chat and Email Design Guide is intended for engineers, system architects, and other technical audience responsible for planning the deployment and maintenance of Enterprise Chat and Email for Cisco Unified Contact Center Enterprise (Unified CCE).

The document is designed to provide sizing guidelines, load-balancing options, network latency considerations, firewall considerations, and interface boundaries.

For sizing guidelines for servers used in the Unified CCE deployment, refer to the Unified CCE SRND guide available here: <http://www.cisco.com/go/srnd>.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at <http://www.cisco.com/cisco/support/notifications.html>

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
<i>Italic</i>	Emphasis. Or the title of a published document.
Bold	Labels of items on the user interface, such as buttons, boxes, and lists. Or text that must be typed by the user.
Monospace	The name of a file or folder, a database table column or value, or a command.
<i>Variable</i>	User-specific text; varies from one user or installation to another.


Document conventions

Other Learning Resources

Various learning tools are available within the product, as well as on the product CD and our web site. You can also request formal end-user or technical training.

Online Help

The product includes topic-based as well as context-sensitive help.

Use	To view
 Help button	Topics in <i>Enterprise Chat and Email Help</i> ; the Help button appears in the console toolbar on every screen.
F1 keypad button	Context-sensitive information about the item selected on the screen.

Online help options

Document Set

The Enterprise Chat and Email documentation is available in the `Documents` folder on the product CD. The latest versions of all Cisco documentation can be found online at <http://www.cisco.com>

The document set contains the following guides:

- ▶ *System Requirements for Enterprise Chat and Email*
- ▶ *Enterprise Chat and Email Installation Guide*

- ▶ *Enterprise Chat and Email Browser Settings Guide*

User guides for agents and supervisors

- ▶ *Enterprise Chat and Email Agent's Guide*
- ▶ *Enterprise Chat and Email Supervisor's Guide*

User guides for administrators

- ▶ *Enterprise Chat and Email Administrator's Guide to Administration Console*
- ▶ *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*
- ▶ *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*
- ▶ *Enterprise Chat and Email Administrator's Guide to Email Resources*
- ▶ *Enterprise Chat and Email Administrator's Guide to Reports Console*
- ▶ *Enterprise Chat and Email Administrator's Guide to System Console*
- ▶ *Enterprise Chat and Email Administrator's Guide to Tools Console*

1

Sizing Guidelines

- ▶ [Sizing Inputs](#)
- ▶ [Planning for Database Growth](#)
- ▶ [About Deploying on Virtual Servers](#)
- ▶ [Sizing for Combined Email, Web, and Voice Scenarios](#)
- ▶ [Additional Configurations for Sizing](#)

Sizing Inputs

Configurations presented in the following sections provide sizing for standardized agents who handle up to 6 email messages per hour, or one chat session at a time. If agents are expected to handle more than 6 email messages per hour, on average, or more than one chat session at a time, convert the agent count into a standardized agent count using the following formula:

Email:

```
Standardized agent count for email = Actual agent count * Average number of
messages handled per hour by each agent / 6
```

Chat:

```
Standardized agent count for chat = Actual agent count * Average number of
concurrent chat sessions handled by each agent
```

Email and Chat:

```
Standardized agent count = Standardized agent count for email + Standardized
agent count for chat
```

Use the standardized agent count to find the appropriate configuration to fit your needs. For sizing for Combined Email, Chat, and Voice Scenarios, see [page 11](#).



Important: The number of concurrent agents per application server cannot exceed 400, as this is the maximum number of concurrent agents that can be supported for email and chat by one ECE server in a Packed CCE deployment of ECE.

Planning for Database Growth

The following factors are considered for calculating the rate of growth of database.

- ▶ Incoming and outgoing email volume per month.
- ▶ Number of email attachments
- ▶ Average size of each email (KB).

The following formula can be used to compute the approximate rate of growth of the database server (MB) per month for activities of type email:

```
((Number of incoming and outgoing emails per month * 2) * (6 + (Average size of
each email message in KB * 2)) / 1024
```

If your system receives emails with attachments, use the following formula and add it to the value for emails.

```
((Number of emails per month with attachments * Average size of attachments
(K)) / 1024)
```

For example, if average volume of incoming and outgoing emails with attachments is 50,000, and average size of each attachment is 5 KB, monthly rate of growth can be computed as:

```
((50,000 * 5) / 1024) = 245 MB per month
```

The following formula can be used to compute the approximate rate of growth of the database server (MB) per month for activities of type chat or callback:

$((\text{Number of incoming and outgoing chat messages per month}) * (6 + (\text{Average size of each chat message in KB} * 3 * 2))) / 1024$



Important: These formulas are meant to be used to plan for database growth. Values arrived at using computation may not be an exact match to actual sizes

Note about archiving:

In deployments that use the Standard edition of Microsoft SQL Server, archive jobs for archiving activities older than a certain number of days must be configured via the Administration Console.

About Deploying on Virtual Servers

All components in the ECE deployment must be installed on virtual servers that utilize the OVA templates available on the DocWiki for proper sizing and resource utilization.

For details see <http://docwiki.cisco.com/wiki>. Locate the page for Unified Communications Virtualization Downloads (including OVA/OVF Templates), and navigate to the section for Enterprise Chat and Email. Note that deployments using the Enterprise edition of SQL Server can expand the size of the database server disk to support growth in data over time.

Since the application leverages the partitioning capabilities of the enterprise editions, data is not archived and purged from the databases. For details about increasing the disk size, see “[Expanding the Disk Size on Database Server Machines](#)” on page 16.

For details about implementing a deployment on virtual servers, see <http://cisco.com/go/uc-virtualized>.

Sizing for Combined Email, Web, and Voice Scenarios

ECE can support multiple media, namely, email, chat, and callback. The following combinations of users can be supported on respective configurations described here.

Important Information About Sizing

- ▶ For a distributed deployment, the concurrent load must be spread evenly across all the web-application servers in the cluster.
- ▶ In the sizing configurations described here, dual CPU can optionally be replaced by 2 single core CPUs and a quad CPU can optionally be replaced by a 4 single core CPUs.
- ▶ Sizing is not affected by the existence of a firewall between the web server and the application server, and by whether the web and application servers are collocated or not.

- ▶ In deployments of 400 or fewer agents, active data must not exceed 110 GB. Deployments using the Standard edition of Microsoft SQL Server must configure archiving to ensure that data is maintained below this size. In deployments with the Enterprise edition, the application leverages the partitioning capabilities of SQL Server, so no specific action—other than increasing the disk space as needed—is required to manage data growth.

Support for up to 400 Standardized Concurrent Agents

Support for up to 400 concurrent agents handling email, chat, or callback, where each agent can work on emails at the rate of 6 emails per hour, or work on a single active chat or callback session, at the rate of 6 chat sessions per hour. Configuration supports an incoming email rate of up to 120,000 emails per month.

In ECE, any combination of agent-customer chat sessions, callback sessions, and email activities agents totaling to 400, can be supported on a two-server configuration consisting of one web server, and another server with the web, application, file, messaging, services, and database components.

This configuration also requires two workflow processes and instances to be configured in the application. For details see the *Enterprise Chat and Email Administrator's Guide to System Console*.

To deploy this configuration, use the following OVA template:

- ▶ `ECE_11.5_400_Win2012_vmv9_v1.0.oVA`



Important: Use this configuration in deployments with Packaged CCE

Support for 401 to 1500 Standardized Concurrent Agents

Support for 401 to 1500 concurrent agents handling email, chat, or callback, where each agent can work on emails at the rate of 6 emails per hour, or work on a single active chat or callback session, at the rate of 6 chat sessions per hour.

This is supported on a configuration consisting of five web servers, five application servers, one file server, one messaging server, one services server, and one database server. Load must be evenly distributed across the web-application servers.

This configuration also requires two workflow processes and instances to be configured in the application. For details see the *Enterprise Chat and Email Administrator's Guide to System Console*.

To deploy this configuration, use the following OVA template:

`ECE_11.5_1500_WIN2012_VMV9_V1.0.OVA`



Important: This configuration cannot be used in deployments with Packaged CCE

Additional Configurations for Sizing

Changes on Web Servers

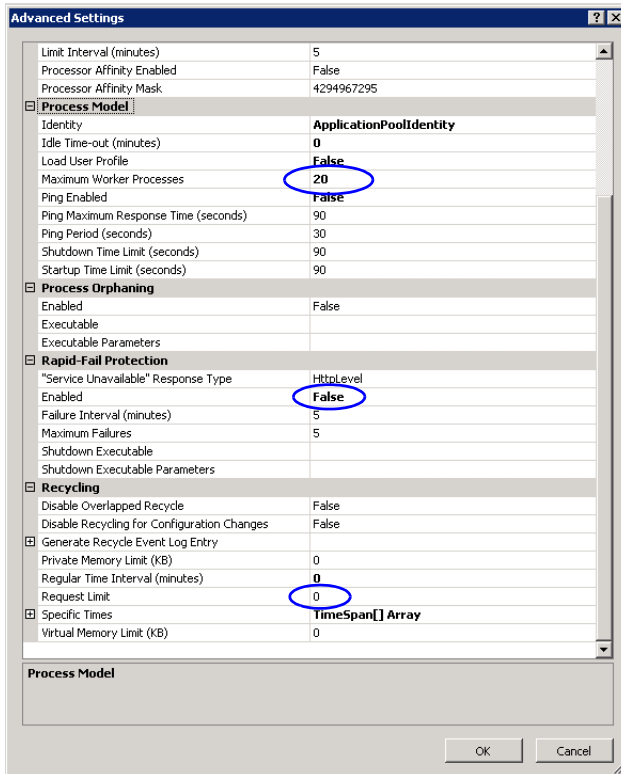
Perform these tasks on all web servers in the deployment.

Updating Default Application Pool Settings

To update the default application pool settings:

1. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the Internet Information Services (IIS) Manager window, browse to *Server_Name* > **Application Pools**.
3. In the Application Pools section, Right-click **DefaultAppPool** and from the menu select, **Advanced Settings**.
4. In the Advanced Settings window, set the following:
 - a. In the **Process Model** section, set:
 - **Maximum Worker Processes** to **20**
 - **Ping Enabled** set to **False** (default value is False)
 - b. In the **Rapid-Fail Protection** section, set:
 - **Enabled** to **False** (default value is False)
 - c. In the **Recycling** section, set:
 - **Request Limit** to **0** (default value is 0)

Click **OK** to close the window.

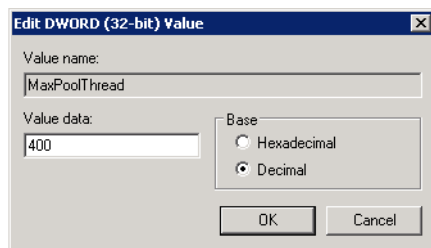


Set the advanced settings

Updating Registry Settings

To update the registry settings:

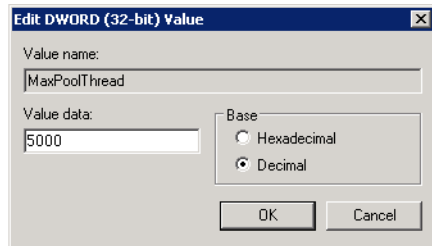
1. Go to Run and type **regedit** to launch the Registry Editor.
2. In the Registry Editor, browse to **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > services > InetInfo > Parameters**.
3. From the parameters list, right-click **MaxPoolThread** and from the menu select **Modify**.
4. In the Edit DWORD (32-bit) Value window, set the **Value data** to **400**.



Set the value to 400

5. In the Registry Editor, browse to **HKEY_LOCAL_MACHINE > Software > Microsoft > ASP.NET > 2.0.50727.0**.

6. In the list section, right-click and from the Menu select **New > DWORD (32-bit) Value**.
7. Name the new **DWORD** as **MaxConcurrentRequestsPerCPU**.
8. Right-click **MaxConcurrentRequestsPerCPU** and from the menu select **Modify**.
9. In the Edit DWORD (32-bit) Value window, set the **Value data** to **5000**.

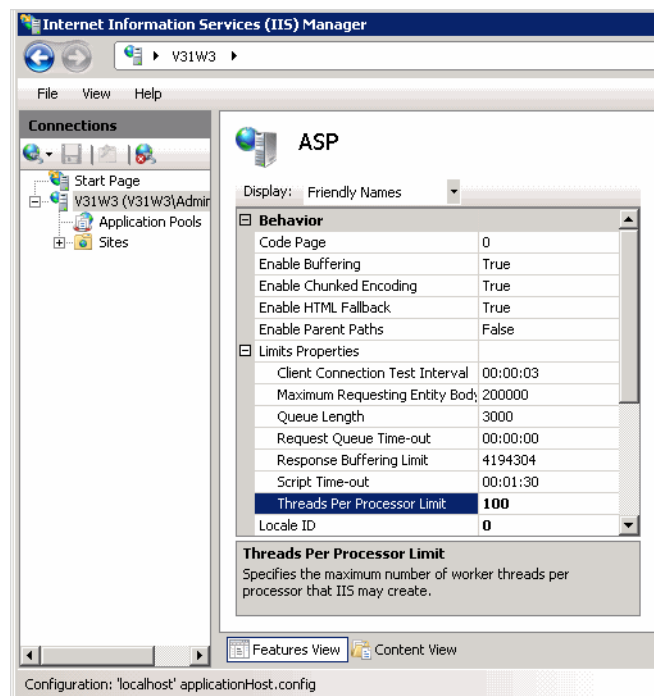


Set the value to 5000

Updating ASP Settings

To update the ASP setting:

1. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the Internet Information Services (IIS) Manager window, browse to *Server_Name*.
3. In the IIS section, right-click **ASP** and from the menu select, **Open Features**.
4. In the properties screen that opens, go to the Limit Properties section and for the **Thread Per Processor Limit** setting, set the value to **100**.

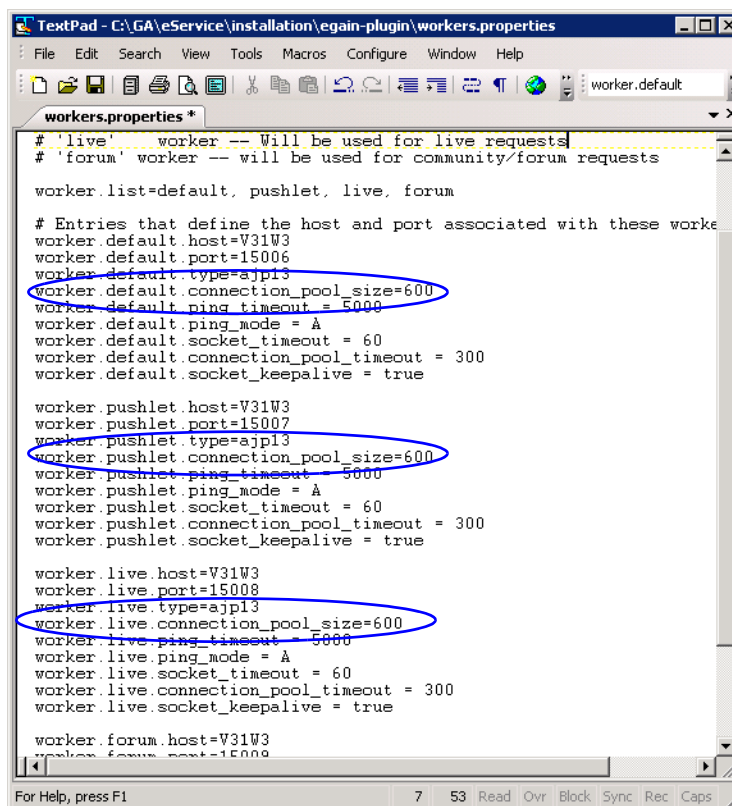


Set the thread per processor limit

Updating the Worker.Properties File

To update the worker.properties file:

1. On the web server, browse to `Cisco_Home\eService\installation\egain-plugin`.
2. Open the `worker.properties` file in a text editor and make the following changes:
 - a. Locate the `worker.default` section in the file and add the following line to this section:
`worker.default.connection_pool_size=600`
 - b. Locate the `worker.pushlet` section in the file and add the following line to this section:
`worker.pushlet.connection_pool_size=600`
 - c. Locate the `worker.live` section in the file and add the following line to this section:
`worker.live.connection_pool_size=600`



```
TextPad - C:\GA\eService\installation\egain-plugin\workers.properties
File Edit Search View Tools Macros Configure Window Help
workers.properties *
# 'live' worker -- Will be used for live requests
# 'forum' worker -- will be used for community/forum requests

worker.list=default, pushlet, live, forum

# Entries that define the host and port associated with these workers
worker.default.host=V31W3
worker.default.port=15006
worker.default.type=ajp13
worker.default.connection_pool_size=600
worker.default.ping_timeout = 5000
worker.default.ping_mode = A
worker.default.socket_timeout = 60
worker.default.connection_pool_timeout = 300
worker.default.socket_keepalive = true

worker.pushlet.host=V31W3
worker.pushlet.port=15007
worker.pushlet.type=ajp13
worker.pushlet.connection_pool_size=600
worker.pushlet.ping_timeout = 5000
worker.pushlet.ping_mode = A
worker.pushlet.socket_timeout = 60
worker.pushlet.connection_pool_timeout = 300
worker.pushlet.socket_keepalive = true

worker.live.host=V31W3
worker.live.port=15008
worker.live.type=ajp13
worker.live.connection_pool_size=600
worker.live.ping_timeout = 5000
worker.live.ping_mode = A
worker.live.socket_timeout = 60
worker.live.connection_pool_timeout = 300
worker.live.socket_keepalive = true

worker.forum.host=V31W3
worker.forum.port=15009
```

Configure the worker properties

Expanding the Disk Size on Database Server Machines

If your deployment uses the enterprise edition of SL Server, over time as the data in your databases grows, you will need to increase the disk space on the database server machines. Follow the instructions provided by VMWare to increase the size of the disk on all the machines on which the data files for the active, master, and reports databases are installed.

Before you increase the disk space, complete the following tasks

- ▶ Stop the application

- ▶ Stop SQL Server

Now expand the disk space on the server where the data size following the VMWare guidelines for your particular operating system. Additional information is available here:

http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1004071

After you expand the size, complete the following tasks

- ▶ Restart the Windows server
- ▶ Log in to the database server where the data files reside and ensure that the disk space has been expanded to the new and increased size
- ▶ Restart SQL Server
- ▶ Restart the application on all the servers in the deployment

Fault Tolerance and Redundancy

- ▶ [Load Balancing Considerations](#)
- ▶ [High Availability Options](#)
- ▶ [Managing Failover](#)

To optimize resource utilization and enhance performance, access to the application can be set up for fault tolerance and redundancy. This chapter discusses some considerations for load-balancing and for configuring systems to achieve high-availability and failover.

Note that the contents of this chapter do not apply to deployments with Packaged CCE.

Load Balancing Considerations

The web service component of a ECE deployment can be load-balanced to serve large number of agents accessing the application at the same time. The web (or web-application) servers can be configured behind the load balancer with a virtual IP address, and a user can access ECE through this IP address. Depending on the load balancing algorithm set, the load balancer will send a request to one of the web-application server behind it and send a response back to the agent. This way, from a security perspective, the load balancer serves as a reverse proxy server too.

One of the most essential parameters while configuring a load balancer is to configure it to support sticky sessions with cookie based persistence. After every scheduled maintenance task, before access is opened for users, it is advised to verify that all web-application servers are available to share the load. In absence of this, the first web-application server could be overloaded, due to the sticky connection feature. With other configurable parameters, one can define load balancing algorithms to meet various objectives such as equal load balance, isolation of a web-application server, or sending lesser requests to a low powered web-application servers.

The load balancer monitors the health of all web-application servers in the cluster, and if a problem is observed, the load balancer removes the given web-application server from the available pool of servers, thus preventing new web requests from being directed to the problematic web-application servers.

High Availability Options

Based on typical customer deployment scenarios, the following recommendations apply towards achieving a high-available system deployment.

Aspect	Description	Advantages
Load Balancer	The load balancer is used for distributing web requests across different web servers. Various types of load balancers are available in the industry. Each of these could be configured with different options work distribution, handling failures, or increased activity.	<ul style="list-style-type: none">▶ Helps distribute load across different servers.▶ Helps configure load distribution based on server capacity and current server resources.▶ Helps handle failures by alternate means of routing a web request.
High-Speed Dedicated LAN	The network is a key ingredient to a successful and highly available application. All ECE servers must be located within the same LAN, and not span over other network domains, to ensure good response times.	<ul style="list-style-type: none">▶ Stable network connections for distributed components.▶ Helps serve web requests in a more predictable and reliable manner.▶ Less delay in responses and thereby increases user experience.
Configuring more than one web-application server	It is highly recommended that more than 1 web-application server be configured. The load balancer detects web server failures and redirects requests to other available web servers, after which, users will have to re-login to the application and a new user session will be created on the target web server.	<ul style="list-style-type: none">▶ More than one web-application server helps to load balance web requests to multiple servers based on both system load and availability of servers.▶ Helps the system scale better to meet growing needs of the enterprise.
Using VMware High Availability options	Deployments can benefit from the features of VMware High Availability (VMHA). For details about virtual server support, see http://cisco.com/go/uc-virtualized For details about VMware High Availability, see the VMHA documentation.	<ul style="list-style-type: none">▶ Removes single points of failure from the deployment.

Recommendations for high availability needs

In addition to these recommendations, if a load balancer is configured to monitor the health of web-application servers, it also serves the purpose of high availability.

Managing Failover

Enterprise Chat and Email supports SQL Server clustering for the database server. Some of the key methods of handling failure conditions within an ECE and Unified CCE integrated deployment are listed here.

- ▶ **Web and Application Servers:** Multiple web-application servers can be deployed in any distributed server deployment. If any of the web-application servers go down, a load balancer can help handle the failure through routing requests to alternate web-application servers. The load balancer detects application server failure and redirects requests to another application server. Users can log into the application without experiencing any significant loss of productivity.

Also note that in deployments without a loadbalancer, if one or more application servers crash, the entire application does not need to be restarted. Only the affected application servers have to be restarted. The rest of the application continues to function normally.

- ▶ **Database Server:** ECE is certified with the edition of SQL Server that supports clustering. If the database server is enabled with Microsoft SQL Server clustering, a primary and secondary database instance will be managed automatically by the cluster for the given database. In the event of a failure to the primary database instance, the secondary database instance will automatically become active. A replication job must be configured by a DBA to periodically keep the primary and secondary database nodes synchronized with the latest data. If SQL Server clustering is not enabled, and the database server goes down, when the database server comes back up, the ECE services automatically reconnect to the database.

The clustering ability of this edition allows adding additional database failover capabilities to a configuration to boost the availability of SQL Server.

Note that this capability is different from splitting the different ECE databases (active, master, archive, etc.) across different machines. In deployments where each of these databases is installed on a separate machine, clustering can be used on each machine to achieve failover for that particular database.

- ▶ **File, Services and Messaging Servers:** ECE is certified with VMware versions that support VMware High Availability. When VMware HA is configured, automatic failover is managed by VMware.
- ▶ **Unified CCE components:** The deployment can allow application services to failover with duplex Unified CCE components (e.g., MR PIM of MR PG and CTI Server of CTI Gateway) to eliminate downtime of the application in failure circumstances.

3 Network Latency

- ▶ [Network Latency](#)
- ▶ [Bandwidth Requirements](#)
- ▶ [Geographic Server Distribution](#)

Note that the contents of this chapter do not apply to deployments with Packaged CCE.

Network Latency

Like any web-based application, set up Enterprise Chat and Email in a high-performance network environment that has sufficient bandwidth with low latency. If the network conditions degrade, it could have an undesirable impact on application performance. Listed here are mandatory guidelines to reduce network latency:

- ▶ Servers which are part of ECE must be connected on the same ethernet switch / VLAN.
- ▶ When agents connect to the application remotely, the permissible network latency is 300 milliseconds (one way). Higher latency between the agents and the applications servers could lead to slower performance on the agent interface.
- ▶ The maximum permissible one-way network delay between the ECE servers and the Unified CCE servers is 300 milliseconds.

It is also important to note that bandwidth is also related to what the user perceives as good performance. For example, one typical “operation” within the application may take n seconds to complete with certain bandwidth, and it may take $n - m$ seconds to complete, if the available bandwidth is more. In both cases, application is usable, although one user perceives it to be faster than the other.

Bandwidth Requirements

The minimum required network bandwidth for an agent connecting to the ECE servers at login is 384 kilobits/second or higher. After login, at a steady state, an average bandwidth of 40 kilobits/second or higher is required.

An attachment size of up to 50 KB can be accommodated within this required bandwidth. For attachments of size greater than 50 KB, temporary slowness may be experienced in the agent user interface during download of the attachments.

Geographic Server Distribution

ECE does not provide support for geographical distribution of ECE application components. However, all Unified CCE components such as the Agent PG may be geographically distributed. The network latency each way between the ECE servers and the Unified CCE components must be ≤ 300 milliseconds in order to ensure optimal communication between ECE and the geographically distributed Unified CCE components.



Firewall and Hardening

- ▶ [Firewall Considerations](#)
- ▶ [Server Hardening Considerations](#)

This chapter discusses some of the firewall and hardening considerations that are useful for Enterprise Chat and Email.

Note that the contents of this chapter do not apply to deployments with Packaged CCE.

Firewall Considerations

- ▶ For agents to access Enterprise Chat and Email, the HTTPS (for secured connections) port needs to be opened at the firewall.

Considerations of applying firewall rules may vary depending on the security policies in effect. If a web server is configured within the firewall with access to the file server ports, Port 139 or 445 to the file server can be blocked from outside the firewall.

- ▶ In a typical installation where agents using Enterprise Chat and Email could be spread across multiple locations, the load balancer, along with the Enterprise Chat and Email web servers, may be deployed in a DMZ. This is a required deployment for installations where customers enter chat sessions from outside the intranet. However, having the web-application servers within the intranet is possible, too. The services and database server can reside in the network over the same or different VLAN.

If integration of these servers is implemented with Active Directory, then associated ports should be opened for communication with Domain Controllers.

Server Hardening Considerations

Dual strategies could be implemented towards securing the application. The first includes implementing standard best practices for physical and software level access controls. These steps could typically be at the corporate level. The other measure is hardening of the server OS and its service components. Please obtain Cisco Security Agent (CSA) with certified security profiles from <http://www.cisco.com> for all the ECE servers to enable intrusion detection and prevention features. For details about the version of CSA that you can use with the application, see the *System Requirements for Enterprise Chat and Email*.

Cisco Security Agent

Cisco Security Agent provides threat protection for servers, also known as endpoints. It identifies and prevents malicious behavior, thereby eliminating known and unknown (“day zero”) security risks and helping to reduce operational costs. The Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, operating system integrity assurance, and audit log consolidation (in managed mode), all within a single product.

Unlike antivirus applications, Cisco Security Agent analyzes behavior rather than relying on signature matching, but both remain critical components to a multi-layered approach to host security. Cisco Security Agent should not be considered a substitute for antivirus applications.

Deploying Cisco Security Agent on Enterprise Chat and Email components involves obtaining a number of application-compatible agents and implementing them according to the desired mode.

For more information on CSA, please go to <http://www.cisco.com>

Default Windows and IIS Service Requirements for ECE

- ▶ *In Accessories*, No Document Templates, No Mouse Pointers.
- ▶ *In Communications*, No Hyper Terminal.
- ▶ *In Application Server*, No Application Server Console, No ASP.NET, No Enable network DTC access, No Message Queuing, IN IIS, No BITS, NO FTP, No FrontPage, No Internet Printing, No NNTP, No, SMTP, In WWW, only WWW Services.
- ▶ No Certificate Services
- ▶ No Email and Fax Services
- ▶ No Indexing Services
- ▶ No Networking Services
- ▶ No Other Network Files & Print Services
- ▶ No Security Configuration Wizard
- ▶ No Terminal Server
- ▶ No Terminal Server Licensing
- ▶ No UDDI
- ▶ No Windows Deployment
- ▶ No Windows Media Services
- ▶ *In Management & Monitoring Tools*, Only SNMP

Guidelines for Microsoft SQL Server

- ▶ Restrict windows authentication user to access .mdf and .ldf files and assign read/write access to appropriate users.
- ▶ Use NTFS file system as it provides advanced security and recovery features.
- ▶ Rename the Windows Administrator account on the SQL Server server to discourage hackers from guessing the administrator password.
- ▶ Hide SQL Server service from appearing in the server enumeration box in Query Analyzer, using the /HIDDEN: YES switch of NET CONFIG SERVER command.
- ▶ Disable Windows guest user account on production servers.
- ▶ Setup roles in SQL Server and configure permissions for windows authentication. Take advantage of the fixed server and database roles by assigning users to the appropriate roles.
- ▶ Restrict access to the SQL logs directory.
- ▶ Secure registry by restricting access to SQL Server registry keys like `HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer`.
- ▶ Encrypt User Views, Stored procedure, Functions, and triggers while going live.

- ▶ Examine the audit for login failure events and look for trends to detect any possible intrusion.