System Users and System User Authentication

Revised: July 25, 2015

Types of System Users

There are two types of users that the user/site administrator can manage. Each type of user is described below.

Care Team Users (providers)

The Extended Care sample portal groups all care team members under the category of *providers*. This includes doctors, nurses, and other healthcare specialists or staff members who will be granted access to the collaboration services and healthcare resources provided by Extended Care.

The user/site administrator is a provider who is assigned a special role within the system to administer both healthcare resources and user access for providers and patients. More than one user/site administrator may exist.

Note The user/site administrator screens in the sample portal refer to the user/site administrator as the *Site Administrator.*

All providers must be granted authorization to access the system before they can use it. The process of identifying and authorizing a system user is called "authentication."

Your role as user/site administrator may involve some level of provider training or advice regarding use of the system. To learn more about the Extended Care provider experience, consider the following.

- You may refer to the *Provider Guide for Extended Care 1.1 Sample Portal*, which is available on the Extended Care product page on www.Cisco.com.
- If your organization is set up for Dedicated authentication of system users, you can setup a provider test account for yourself and explore the provider experience that way.

Note Screens in the Extended Care sample portal refer to providers as *users*.
To eliminate confusion, this document will use the following terms.
Providers = care team members and user/site administrators
System users = all users of the system, including *patients* and providers

Patients

Just like your providers, patients must be authenticated prior to gaining access to the system.

Your role as user/site administrator may involve some level of patient training or advice regarding use of the system. To learn more about the Extended Care patient experience, you may refer to the *Patient Guide for Extended Care 1.1 Sample Portal*, which is available on the Extended Care product page on www.Cisco.com.

Other System Access Accounts

There are other people in your healthcare organization that will be able to access not only the Extended Care sample portals, but also the Extended Care application server that controls the portals and how they are configured and supported. These administrator accounts manage the Extended Care application server and resource connectors the application server uses to provide external healthcare resources to the sample portals. The Extended Care Server Administrator, in particular, is assigned special privileges to setup and configure the Extended Care application server. Your organization will decide what system features will be available for your organization and this administrator will set up the portals accordingly.

For more information on the administrator roles and workflow, you may refer to the *Server Installation and Administration Guide for Extended Care 1.1*, which is available on the Extended Care product page on www.Cisco.com.

Extended Care Connector Administrator

The connector administrator is assigned special privileges to setup and configure the Extended Care connectors, whcih provide , as well as the connectors the application server uses to provide external healthcare resources to the sample portals. Your organization will decide what system features will be available for your organization and the server administrator will set up the portals accordingly. **The user/site administrator has no control over server administrator access to the system.**

To learn more about the Extended Care server administrator workflow:

- You may refer to the *Server Installation and Administration Guide for Extended Care 1.1*, which is available on the Extended Care product page on www.Cisco.com.

Authorizing User Access (authentication)

All system users must be granted access authorization to the system before they can use it. When establishing a new system user account, specific data (typically a user name and password) is used to verify the identity of the user, for the purpose of granting that access. The process of using that data to verify identity is called "authentication”. Your organization determines which authentication modes they will use when they do their implementation planning. Your Extended Care server administrator will select the authentication mode during the Extended Care installation process outlined in the *Server Installation and Administration Guide for Extended Care 1.1.*

The Extended Care authentication database stores all authentication data that is required by Extended Care for both providers and patients. The following Extended Care authentication modes determine how that data is loaded into the Extended Care authentication database.

Note As a security precaution, the user/site administrator account is always authenticated against the local Cisco database, regardless of the mode of authentication used for other user accounts. This account is also not locked out for account inactivity.

Provider Authentication: Including User/Site Administrators

Dedicated (internal) Authentication Mode

With this type of authentication, all usernames, passwords, and user attributes are manually entered into a Extended Care database. This allows special user IDs to be created ad hoc for training purposes or perhaps for temporary employees. It also allows an enterprise to utilize the training and testing user names that ship with the product, regardless of how other users will be authenticated.

Note No method is built into the sample portals to bulk load provider authentication data.However, an integration tool is available to accomplish this. To use this tool, your organization should contact their Cisco Extended Care account representative and inquire about the *User On-Boarding API tool*.

Security Options

The security options described here are ***only*** available to sites that use the Dedicated authentication mode and the Mixed authentication mode. How these options are implemented is determined when the Cisco Extended Care software is installed. The user/site administrator cannot change these settings (but the Extended Care server administrator can). They are described here so that you can answer questions from the users, if necessary.

These are the options and their default settings:

- Forced Password Change – Required with first log in.
- Account Inactivity – Disable or Lock out after ninety days.
- Strong Passwords – Configurable minimum number of characters or types of symbols.
- Password Expiration – After ninety days.
- Password Reuse – Checks last four passwords.
- User Lockout – After six unsuccessful attempts.

Forced Password Change

By default, when a new user account is created or when the password is changed by the Site Administrator, the user must change the account password the first time that he or she logs into the application. This feature can be turned off.

Account Inactivity

By default, accounts that have been inactive for ninety days will be automatically disabled. The Site Administrator must unlock the account before it can be used. This feature can be turned off, and the inactivity time can be configured when the application is installed. This policy is not applied to the Site Admin account.

Strong Passwords

By default, passwords must be at least seven characters long, and must include at least two character types (upper case, lower case, numbers, symbols). This policy can be turned off, and the minimum length and minimum number of characters types can be configured.

Password Expiration

By default, passwords will expire and have to be changed after ninety days. This feature can be turned off, and the expiration time can be configured.

Password Reuse

By default, the application saves four old passwords, and does not allow the user to use them again. This feature can be turned off, and the number of saved passwords can be configured.

User lockout

By default, after six unsuccessful login attempts an account will be locked. The Site Administrator can unlock these accounts. This policy can be turned off, and the number of unsuccessful login attempts can be configured.

The impacts of the available authentication modes are described below.

External (dynamic update) Authentication Mode

This supports the authentication of users by referencing an external directory maintained by or for your organization. This allows an enterprise to maintain a single user name and password for access to Cisco Extended Care and all their other resources. Two types of directories are supported.

External LDAP

This type of authentication references directories that support both the LDAP and LDAPS Lightweight Directory Access Protocol. Only the user's LDAP ID is stored in Extended Care. When authentication is required, Extended care references the LDAP directory for authentication. When users change their passwords on the external directory, the same password works for access to Cisco Extended Care.

External Connector (non-LDAP)

This is a connector-based process that allows third-party EMR/PHR applications and Cisco Extended Care to use a common (non-LDAP) directory to authenticate users. Extended Care fetches the demographic information from the third-party application and stores it in an Extended Care database.

Note No method is built into the sample portals to bulk load provider authentication data. However, an integration tool is available to accomplish this. To use this tool, your organization should contact their Cisco Extended Care account representative and inquire about the User On-Boarding API tool.

Mixed LDAP

When this mode is configured, the user/site administrator may register and authenticate a user using either the manual Dedicated Mode or by referencing an LDAP directory.

Mixed Connector

When this mode is configured, the user/site administrator may register and authenticate a user using either the manual Dedicated Mode or by fetching data from third-party EMR/PHR application.

Note There are special security options that are available for both forms of Mixed authentication. See "Security Options" on page 2-3

Patient Authentication

Patients may only be registered and authenticated using an external connector. This connector-based process allows third-party EMR/PHR applications and Cisco Extended Care to use a common (non-LDAP) directory to authenticate users. Extended Care fetches demographic information from the third-party application and stores it in the Extended Care authentication database.

Note No method is built into the sample portals to bulk load patient authentication data. However, an integration tool is available to accomplish this. To use this tool, your organization should contact their Cisco Extended Care account representative and inquire about the *User On-Boarding API* tool.

Server Administrators and Connector Administrators

Authentication data for both of these system administrator users is stored in the Extended Care authentication database, which is associated with Dedicated authentication. It is not your responsibility nor are you given the capability to manage these users.

Summary of Authentication Options

Table 2-1 Summary of Authentication Options

User	**Dedicated** (Add/Delete)	**External LDAP** (Enable/Disable)	**External Connector /non-LDAP** (Enable/Disable)	**Mixed LDAP**	**Mixed Connector** (non-LDAP
Patient	No	No	Yes	No	No
Provider	Yes	Yes	Yes	Yes	Yes
Server Admin	Yes	No	No	No	No
Connector Admin	Yes	No	No	No	No