Configuration - Two-Factor Countdown

Summary

LSPs requested a notification web page for users as they are added to required Two-Step cohorts with information messages regarding when the user will be required, how to enroll, and any additional information the user may need.

Requirements

The web page should come from the idp.pennkey.upenn.edu server and not from the weblogin.pennkey.upenn.edu server because we are deprecating that domain in the near future and do not want to waste this effort.

The web page should match look and feel of the existing weblogin authentication pages.

The web page should not be too annoying about the warning message or occur too frequently.

The web page should notify the user how many days until two-step enforcement becomes mandatory.

The web page should provide links to enroll in two-step, additional info about two-step, and the ability to proceed.

Implementation

Summary

The proposed solution to this problem is to utilize Shibboleth Identity Provider v3.3.3 intercepts feature combined with PennGroups entitlements to show a distinct two-step warning screen to users.

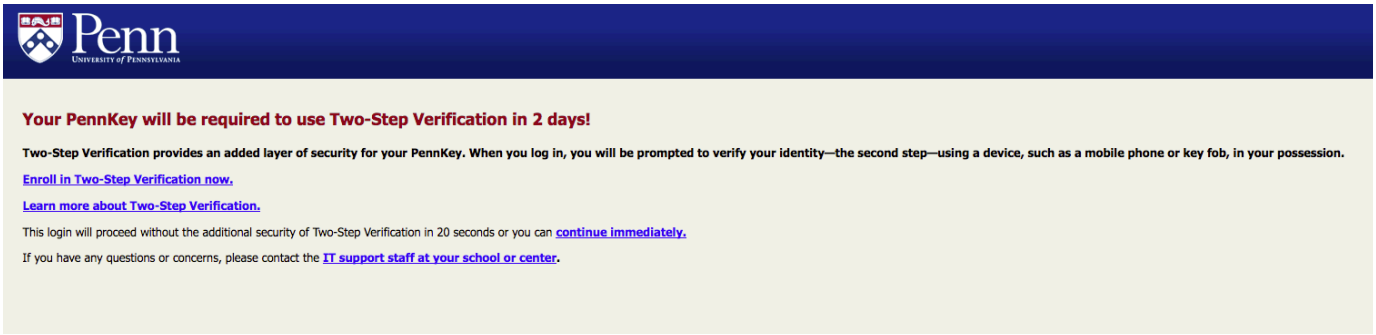
If a request is submitted to increase this function to 10+ days, incrementing the token 'idp.login.twoStepGroupMax' in idp.home/messages/messages.properties will achieve this effect.

Additions to the edit-webapp directory require rebuilding the idp.war file.

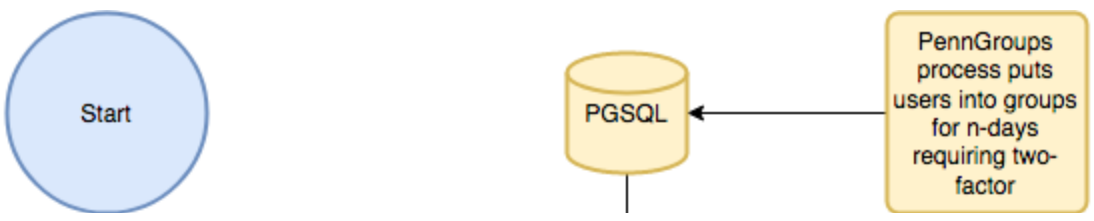
Deployment

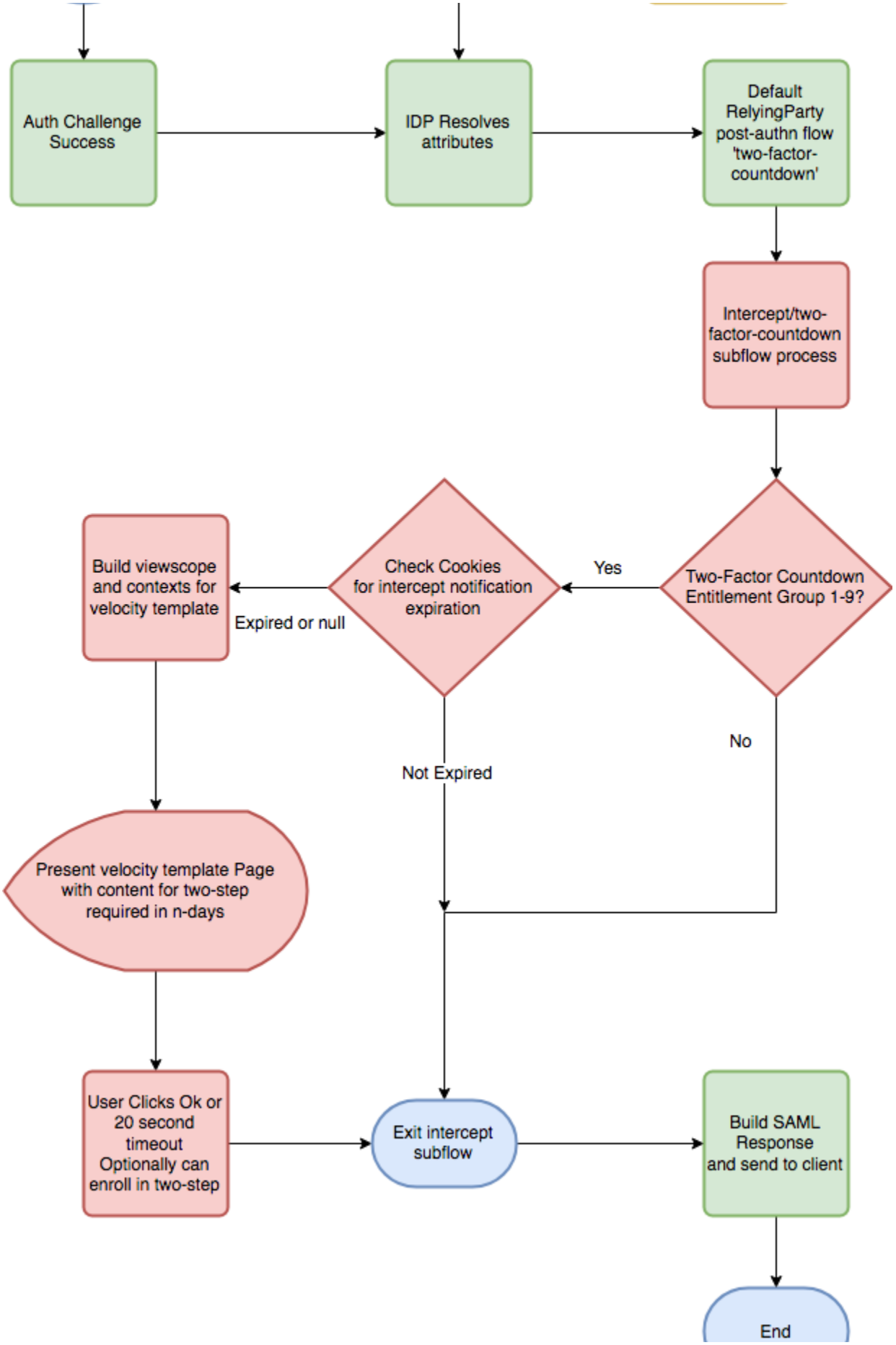
Deployment steps Two-Factor-Countdown

Result



Process Flow




Auth Challenge Success
IDP Resolves attributes
Default RelyingParty post-authn flow 'two-factor-countdown'
Intercept/two-factor-countdown subflow process
Two-Factor Countdown Entitlement Group 1-9?
Yes
Check Cookies for intercept notification expiration
Expired or null
Build viewscope and contexts for velocity template
No
Not Expired
Present velocity template Page with content for two-step required in n-days
User Clicks Ok or 20 second timeout Optionally can enroll in two-step
Exit intercept subflow
Build SAML Response and send to client
End

Intercept

Files

- conf/intercept/profile-intercept.xml
- conf/intercept/two-factor-countdown-config.xml (New file)
- views/intercept/two-factor-countdown.vm (New file)
- flows/intercept/two-factor-countdown/two-factor-countdown-flow.xml (New file/directory)
- flows/intercept/two-factor-countdown/two-factor-countdown-beans.xml (New file/directory)
- messages/messages.properties
- conf/relying-party.xml
- edit-webapp/css/countdown.css
- edit-webapp/images/portal_penn_banner.gif

Profile-intercept.xml

Add new bean id="intercept/two-factor-countdown"

```
<bean id="shibboleth.AvailableInterceptFlows"
parent="shibboleth.DefaultInterceptFlows" lazy-init="true">
        <property name="sourceList">
            <list merge="true">
                <bean id="intercept/context-check"
parent="shibboleth.InterceptFlow" />

                <bean id="intercept/expiring-password"
parent="shibboleth.InterceptFlow" />

                <bean id="intercept/terms-of-use"
parent="shibboleth.consent.TermsOfUseFlow" />

                <bean id="intercept/attribute-release"
parent="shibboleth.consent.AttributeReleaseFlow" />

                <bean id="intercept/two-factor-countdown"
parent="shibboleth.InterceptFlow" />
            </list>
        </property>
    </bean>
```

Two-factor-countdown-config.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:context="http://www.springframework.org/schema/context"
       xmlns:util="http://www.springframework.org/schema/util"
       xmlns:p="http://www.springframework.org/schema/p"
       xmlns:c="http://www.springframework.org/schema/c"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd
                           http://www.springframework.org/schema/context
http://www.springframework.org/schema/context/spring-context.xsd
                           http://www.springframework.org/schema/util
http://www.springframework.org/schema/util/spring-util.xsd"

       default-init-method="initialize"
       default-destroy-method="destroy">

    <!--
    Condition to evaluate to determine if they need to see two-factor
countdown intercept.
    -->
    <bean id="shibboleth.two-factor-countdown.Condition"
parent="shibboleth.Conditions.NOT">
        <constructor-arg>
            <bean
class="net.shibboleth.idp.profile.logic.RegexAttributePredicate"
                p:useUnfilteredAttributes="true"
                p:attributeId="eduPersonEntitlement"

p:pattern="^urn:mace:upenn\.edu:penn:isc:ait:apps:twoFactor:groups:twoFact
orCountdown:twoFactorCountdown_\d*$">
            </bean>
        </constructor-arg>
    </bean>

    <!-- Name of cookie to track when user was last notified. -->
    <bean id="shibboleth.two-factor-countdown.NotifyCookieName"
class="java.lang.String" c:_0="shib_idp_two_factor_countdown" />

    <!-- Interval (milliseconds) between notifications, default is 8 hours.
-->
    <bean id="shibboleth.two-factor-countdown.NotifyInterval"
class="java.lang.Long" c:_0="28800000" />

</beans>
```

Two-factor-countdown.vm

```
##
```

```
## Velocity Template for two step countdown view
##
## Velocity context will contain the following properties
## flowExecutionUrl - the form action location
## flowRequestContext - the Spring Web Flow RequestContext
## flowExecutionKey - the SWF execution key (this is built into the
flowExecutionUrl)
## profileRequestContext - root of context tree
## encoder - HTMLEncoder class
## request - HttpServletRequest
## response - HttpServletResponse
## environment - Spring Environment object for property resolution
##
##
##
##
##
## Velocity code to build the h3 text used below.  This template only
executes when
'penn:isc:ait:apps:twoFactor:groups:twoFactorCountdown:twoFactorCountdown_
N' entitlement is present.
## Variables intialized with fail-safe values in case we get to this
template by accident.
## attributeContext is an object that stores the attributes for this
request context.
## getUnfilteredIdPAttributes method used to get a hashmap of all resolved
attributes before SP filtering occurs from the $attributeContext.
## getValues method returns List<IdPAttribute>
## getDisplayValue method returns the IdPAttribute in string format,
shortcut for getValue().toString().
## springMessageText values found in
{idp.home}/messages/messages.properties

    #set ($whenText = "soon")
    #set ($entitlementsMap =
$attributeContext.getUnfilteredIdPAttributes().get('eduPersonEntitlement')
.getValues())
    #set ($match = false)
 #set ($groupName = "#springMessage('idp.login.twoStepGroupName')")
    #set ($groupMax = 9)
    #set ($groupMax =
$groupMax.parseInt("#springMessage('idp.login.twoStepGroupMax')"))

    #foreach ($i in [1..$groupMax])
        #if ($match)#{break}#end
        #set ($testVal = "$groupName$i")
        #foreach ($value in $entitlementsMap)
            #if ($value.getDisplayValue() == $testVal)
                #set ($match = true)
                #set ($whenText = "in $i #if ($i == 1) day#{else}
days#end")
            #end
        #end
```

```
    #end

<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta name="viewport"
content="width=device-width,initial-scale=1.0">
        <title>#springMessageText("root.title", "Penn WebLogin")</title>
        <link rel="stylesheet" type="text/css"
href="$request.getContextPath()/css/countdown.css">
        <meta http-equiv="refresh"
content="20;url=$flowExecutionUrl&_eventId_proceed=1">
    </head>

    <body>
        <!-- banner -->
        <div id="banner">
            <a href="http://www.upenn.edu/">
                <img
src="$request.getContextPath()#springMessage("idp.logo.small")"
alt="#springMessageText("idp.logo.small.alt-text", "Penn: University of
Pennsylvania")" border="0" width="220" height="82" />
            </a>
        </div>

        <div id="content">

        <h3>#springMessageText("idp.login.twoStepRequiredSoon", "Your
Pennkey will be required to use Two-Step Verification ")${whenText}!</h3>
            <p><strong>#springMessageText("idp.login.twoStepDescription",
"Two-Step Verification provides an added layer of security for your
PennKey. When you log in, you will be prompted to verify your
identity&mdash;the second step&mdash;using a device, such as a mobile phone
or key fob, in your possession.")</strong></p>

            <p>
                <strong><a
href="#springMessageText("idp.login.twoStepEnrollLink",
"https://twostep.apps.upenn.edu/")"
target="_blank">#springMessageText("idp.login.twoStepEnrollText", "Enroll
in Two-Step Verification Now.")</a></strong>
            </p>
            <p>
                <strong><a
href="#springMessageText("idp.login.twoStepInfoLink",
"https://www.isc.upenn.edu/how-to/two-step-faq")"
target="_blank">#springMessageText("idp.login.twoStepInfoText", "Learn more
about Two-Step Verification.")</a></strong>
            </p>
            <p>
                #springMessageText("idp.login.twoStepResponseProceed",
"This login will proceed without the additional security of Two-Step
```

```
Verification in 20 seconds or you can ")
                <strong><a
href="$flowExecutionUrl&_eventId_proceed=1">#springMessageText("idp.login.
proceedButtonText", "continue immediately.")</a></strong>
            </p>
   <p>
                #springMessageText("idp.login.twoStepGetHelp", "If you have
any questions or concerns, please contact the ")
                <strong><a
href="#springMessageText("idp.login.GetHelpLink",
"https://www.isc.upenn.edu/get-it-help")"
target="_blank">#springMessageText("idp.login.GetHelpText", "IT support
staff at your school or center")</a>.</strong>
            </p>
        </div>
    </body>
</html>
```

Two-factor-countdown-flow.xml

```
<flow xmlns="http://www.springframework.org/schema/webflow"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.springframework.org/schema/webflow
http://www.springframework.org/schema/webflow/spring-webflow.xsd"
       parent="intercept.abstract">

    <!-- Rudimentary impediment to direct execution of subflow. -->
    <input name="calledAsSubflow" type="boolean" required="true" />

    <!-- If the condition is true, we don't need to notify, otherwise check
cookie to see if we do. -->
    <decision-state id="CheckContext">
        <if
test="TwoFactorCountdownPredicate.apply(opensamlProfileRequestContext)"
            then="ShouldUnsetCookie" else="CheckCookie" />
    </decision-state>

    <decision-state id="ShouldUnsetCookie">
        <if
test="TwoFactorCountdownCookieManager.getCookieValue(TwoFactorCountdownCoo
kieName, null) != null"
            then="UnsetCookie" else="proceed" />
    </decision-state>

    <action-state id="UnsetCookie">
        <evaluate
expression="TwoFactorCountdownCookieManager.unsetCookie(TwoFactorCountdown
CookieName)" />
        <transition to="proceed" />
```

```
    </action-state>

    <decision-state id="CheckCookie">
        <if test="T(java.lang.System).currentTimeMillis() -
T(java.lang.Long).parseLong(TwoFactorCountdownCookieManager.getCookieValue
(TwoFactorCountdownCookieName, '0')) > TwoFactorCountdownNotifyInterval"
            then="DisplayTwoFactorCountdownView" else="proceed" />
    </decision-state>

    <view-state id="DisplayTwoFactorCountdownView"
view="#{flowRequestContext.activeFlow.id}">
        <on-render>
            <evaluate
expression="TwoFactorCountdownCookieManager.addCookie(TwoFactorCountdownCo
okieName,
T(java.lang.Long).toString(T(java.lang.System).currentTimeMillis()))" />
            <evaluate expression="environment"
result="viewScope.environment" />
            <evaluate
expression="T(net.shibboleth.utilities.java.support.codec.HTMLEncoder)"
result="viewScope.encoder" />
            <evaluate
expression="flowRequestContext.getExternalContext().getNativeRequest()"
result="viewScope.request" />
            <evaluate
expression="flowRequestContext.getExternalContext().getNativeResponse()"
result="viewScope.response" />
            <evaluate expression="opensamlProfileRequestContext"
result="viewScope.profileRequestContext" />
            <evaluate
expression="opensamlProfileRequestContext.getSubcontext(T(net.shibboleth.i
dp.profile.context.RelyingPartyContext),
true).getSubcontext(T(net.shibboleth.idp.attribute.context.AttributeContex
t))" result="requestScope.attributeContext" />
        </on-render>

        <transition to="proceed" />
    </view-state>

    <end-state id="proceed" />
```

```
    <bean-import resource="two-factor-countdown-beans.xml" />

</flow>
```

Two-factor-countdown.beans.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xmlns:context="http://www.springframework.org/schema/context"
       xmlns:c="http://www.springframework.org/schema/c"
       xmlns:p="http://www.springframework.org/schema/p"
       xmlns:util="http://www.springframework.org/schema/util"
       xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd
                           http://www.springframework.org/schema/context
http://www.springframework.org/schema/context/spring-context.xsd
                           http://www.springframework.org/schema/util
http://www.springframework.org/schema/util/spring-util.xsd"

       default-init-method="initialize"
       default-destroy-method="destroy">

    <bean
class="org.springframework.context.support.PropertySourcesPlaceholderConfi
gurer"
        p:placeholderPrefix="%{" p:placeholderSuffix="}" />

    <bean
class="net.shibboleth.ext.spring.config.IdentifiableBeanPostProcessor" />
    <bean
class="net.shibboleth.idp.profile.impl.ProfileActionBeanPostProcessor" />

    <import
resource="../../../conf/intercept/two-factor-countdown-intercept-config.xm
l" />

    <!-- Simplifies flow definition expressions. -->
    <alias name="shibboleth.two-factor-countdown.Condition"
alias="TwoFactorCountdownPredicate"/>
    <alias name="shibboleth.PersistentCookieManager"
alias="TwoFactorCountdownCookieManager" />
    <alias name="shibboleth.two-factor-countdown.NotifyCookieName"
alias="TwoFactorCountdownCookieName" />
    <alias name="shibboleth.two-factor-countdown.NotifyInterval"
alias="TwoFactorCountdownNotifyInterval" />

</beans>
```

Messages.properties

```
# You can define message properties here to override messages defined in
# system/messages/ or to add your own messages.
idp.footer = Copyright 2018 - University of Pennsylvania
root.footer = Copyright 2018 - University of Pennsylvania
idp.logo = /images/portal_penn-banner_lg.gif
idp.logo.alt-text = University of Pennsylvania crest and logo
root.title = Penn WebLogin

# Two-Step Countdown messages
idp.login.twoStepGroupName =
urn:mace:upenn.edu:penn:isc:ait:apps:twoFactor:groups:twoFactorCountdown:t
woFactorCountdown_
idp.login.twoStepGroupMax = 9
idp.login.twoStepRequiredSoon = Your PennKey will be required to use
Two-Step Verification
idp.login.twoStepEnrollText = Enroll in Two-Step Verification now.
idp.login.twoStepEnrollLink = https://twostep.apps.upenn.edu/
idp.login.twoStepInfoText = Learn more about Two-Step Verification.
idp.login.twoStepInfoLink = https://www.isc.upenn.edu/how-to/two-step-faq
idp.login.twoStepDescription = Two-Step Verification provides an added
layer of security for your PennKey. When you log in, you will be prompted
to verify your identity&mdash;the second step&mdash;using a device, such as
a mobile phone or key phone, in your possession.
idp.login.twoStepResponseProceed = This login will proceed without the
additional security of Two-Step Verification in 20 seconds or you can
idp.login.proceedButtonText = continue immediately.
idp.login.twoStepGetHelp = If you have any questions or concerns, please
contact the
idp.login.twoStepGetHelpLink = https://www.isc.upenn.edu/get-it-help
idp.login.twoStepGetHelpText = IT support staff at your school or center
idp.logo.small = /images/portal_penn-banner.gif
idp.logo.small.alt-text = Penn: University of Pennsylvania
```

Relying-party.xml

```
<bean parent="SAML2.SSO" p:encryptAssertions="false"
p:encryptNameIDs="false" p:signResponses="true"
p:postAuthenticationFlows="two-factor-countdown"/>
```

countdown.css

```
body {
    font-family: Tahoma, Arial, Helvetica, sans-serif;
    font-size: 0.80em;
    background-color: #f0f0ea;
    color: #000;
    margin: 0;
    padding: 0;
}

a {
    text-decoration: underline;
}

h3 {
    font-size: 1.40em;
    font-weight: bold;
    color: #95001A;
}

#banner {
    background-image: url(../images/portal_banner4-bg.gif);
}

#content {
    margin-top: 2.6em;
    margin-left: 2em;
    margin-right: 2em;
}
```